Deutsches
Patent- und Markenamt

IT-Sicherheit
im
Deutschen Patent- und Markenamt

Computer-Viren-Schutzkonzept
des
Deutschen Patent- und Markenamtes

Dokumenten-Information

Autor	IT-Sicherheitsmanagement
Stand (letztes Speicherdatum)	29.08.2007 15:27:00
Dateiname und Pfad	Computer_Virenschutzkonzept_des_DPMA_V1.doc
Version	1.0
Freigabestatus	{in Bearbeitung | übergeben | abgenommen}

Änderungsnachweis

Version	Datum	Autor	Änderungen
1	21.10.04	IT-Sicherheit	Ersterstellung

Abkürzungen und Konventionen

Abkürzungen	BSI	Bundesamt für Sicherheit in der Informationstechnik
	DPMA	Deutsches Patent- und Markenamt
	IDS	Intrusion Detection System
	IT-GSHB	IT-Grundschutzhandbuch des Bundesamtes für Sicherheit in der Informationstechnik
Glossar		
Konventionen	Wird im Text die männliche Form verwendet, geschieht dies ausschließlich aus Gründen der leichteren Lesbarkeit.	
Querverweise	[1] Benutzerrichtlinien für den ordnungsgemäßen Einsatz von Personalcomputern im Deutschen Patent- und Markenamt (siehe \\vfshome\it_security\Public\Benutzerrichtlinien\PC-Benutzerrichtlinien.doc)	
	[2] IT-Sicherheit im Deutschen Patent- und Markenamt – Richtlinien und Hinweise für Endanwender (siehe: http://info.dpma.de/h2/Benutzerinformation_IT_Sicherheit.pdf)	
	[3] IT-Sicherheitsrichtlinien Fernwartung und Telearbeit (siehe \\vfshome\it_security\Public\Benutzerrichtlinien\Sicherheitsrichtlinien Fernwartung V1.1.doc	
	[4] Dienstvereinbarung über die Nutzung von Intranet- und Internet-Diensten im Deutschen Patent- und Markenamt (siehe: http://info.dpma.de/h4/Sond10_2001.pdf)	
	[5] IT-Grundschutzhandbuch des Bundesamtes für Sicherheit in der Informationstechnik (siehe: \\maagvs002\IT-GSHB2002\html\menue.htm)	
	[6] Verfügung des Leiters der Hauptabteilung Informationstechnik (H2), Vermerk Az.: 1519 E 10.13 - H 2 vom 28.06.2000: IT-Sicherheitsmanagement - Einrichtung einer zentralen Stelle zur Erfassung IT-sicherheitsrelevanter	

	Ereignisse (siehe: \\vfshome\it_security\Public\Benutzerrichtlinien\Zentrale-Störfallmeldung-VfgH2-280600.doc)
	[7] Vermerk des IT-Sicherheitsmanagement, Az.: 1519/1 E 001 – 2.0.2 vom 10.05.2004: IT-Sicherheit – Flächendeckender Virenschutz (Benennung von Ansprechpartnern in den Fachbereichen)
	[8] Grundsätzliche Regeln zur IT-Sicherheitsmanagement de Deutschen Patent- und Markenamtes vom 08.11.1999, geändert am 14.06.2004-07-08 (siehe: \\vfshome\it_security\Public\Sicherheitspolitik\Sicherheitspolitik.doc)

Inhalt

1. SCHUTZBEDARFSANALYSE 6

1.1 Vorbemerkung 6

1.2 Abhängigkeit des DPMA vom IT-Einsatz 6

1.3 Beschreibung des Gefährdungspotentials 6

1.4 Schadensszenarien 9

1.5 Potentiell betroffene IT-Systeme (M 2.155) 10

1.5.1 Microsoft Windows Betriebssysteme 10
1.5.2 UNIX- und LINUX-Betriebssysteme 11
1.5.3 spezielle Anwendungssoftware 11
1.5.4 Zentraler Fileserver 11
1.5.5 Andere Betriebssysteme 11

2. ERFORDERLICHE SCHUTZMAßNAHMEN 13

2.1 Computer-Virenschutz-Strategie (M 2.156) 13

2.1.1 Infektionswege 13
2.1.2 Einsatz von Virenscannern 14
2.1.3 Viruswall (M 2.157) 15
2.1.3.1 HTTP 15
2.1.3.2 HTTPS 15
2.1.3.3 SMTP (E-Mail) 16
2.1.3.4 Rechtliche Aspekte 16
2.1.3.5 Weitere Sicherheitsmaßnahmen 17
2.1.4 Zentraler E-Mail-Server MS-Exchange (M 2.157) 17
2.1.4.1 Virenschutz 17
2.1.4.2 Rechtliche Aspekte 17
2.1.4.3 Weitere Sicherheitsmaßnahmen 17
2.1.5 Nicht-vernetzte IT-Systeme (M 2.157) 18
2.1.6 Vernetzte Endgeräte (M 2.157) 18
2.1.7 Mobile Geräte (M 2.157) 19
2.1.8 Server (M 2.157) 19
2.1.9 Geräte von Fremdfirmen 19
2.1.10 Weitere Maßnahmen zur Gewährleistung eines flächendeckenden Virenschutzes (M 2.156) 20
2.1.11 Weitere Sicherheitssysteme zum Schutz gegen Computer-Viren (M 2.156) 20
2.1.11.1 Intrusion Detection System 20
2.1.11.2 Trasher 21
2.1.11.3 Analyse der Internetverbindungen (http, https) – System PRPROTOK 22

2.2 Aktualisierung der Computer-Viren-Suchprogramme (M 2.159) 23

2.2.1 Viruswall 23
2.2.2 E-Mail-Server 23
2.2.3 Nicht-vernetzte IT-Systeme 23
2.2.4 Vernetzte Endgeräte 23
2.2.5 Server 23

3. REGELUNGEN 25

3.1 Regelungen zum Schutz vor Computer-Viren (M 2.160) 25

3.1.1 Nutzungsverbot nicht freigegebener Software (M 2.9) 25
3.1.1.1 Geltende Regelung 25
3.1.1.2 Weitere technische Maßnahmen 25
3.1.1.3 Verfahren zur Softwarefreigabe 25
3.1.1.4 Information der Endanwender 25
3.1.2 Überprüfung des Einsatzes nicht freigegebener Software (M 2.10) 26
3.1.2.1 Stichprobenprüfung 26
3.1.2.2 anlassbezogene Prüfungen 26
3.1.3 Dokumentation der Veränderungen an einem bestehenden System (M 2.34) 26
3.1.4 Informationsbeschaffung über Sicherheitslücken der Systeme (M 2.35) 26

3.1.5 Schulung der IT-Benutzer (M 3.4, 3.5) ... 26
3.1.6 Nutzung der BIOS-Sicherheitsmechanismen (M 4.84) ... 27
3.1.7 Erstellen einer Notfall-Diskette (M 6.24) ... 27
3.1.8 Maßnahmen bei nicht-resident virenschutzkontrollierten IT-Systemen ... 27
3.1.8.1 Regelmäßiger Einsatz eines Computer-Viren-Suchprogramms ... 27
3.1.8.2 Virenkontrolle bei Datenträgeraustausch und Datenübertragung ... 27
3.1.8.3 Prüfung eingehender Dateien auf Makro-Viren ... 28
3.1.9 Datenaustausch (M 4.33, 4.44) ... 28
3.1.10 Regelmäßiger Einsatz eines Virensuchprogramms (M 4.3) ... 28
3.1.11 Regelmäßige Datensicherung (M 6.32) ... 28
3.1.12 Eingeschränkte Benutzerumgebung ... 28
3.1.13 Abnahmeprüfung von Servern durch das IT-Sicherheitsmanagement ... 28
3.2 Regelung der Verantwortlichkeiten 29
3.2.1 Ansprechpartner für Computer-Viren ... 29
3.2.2 Verantwortlichkeit von Administratoren ... 30
3.2.2.1 Allgemeine Verantwortung von Administratoren ... 30
3.2.2.2 Systemadministratoren ... 30
3.2.2.3 Viruswall-Administrator ... 31
3.2.2.4 E-Mail-Server-Administration ... 31
3.2.3 Verantwortlichkeit des IT-Sicherheitsmanagements ... 31
3.2.4 Verantwortlichkeit des einzelnen IT-Benutzers ... 31

4. VORGEHEN BEI VIRENVERDACHT ... 32
4.1 Verhalten bei Virenbefall oder -verdacht 32
4.2 Vorgehensweise bei Auftreten eines Computer-Virus (M 2.158, M 6.22) 32
4.3 Meldewege bei Auftreten eines Computer-Virus 33
4.3.1 Allgemeine Regelung ... 33
4.3.2 Meldewege bei Programmen mit Schadenswirkung ... 34

5. HILFSMITTEL ... 35
5.1 Verhaltensregeln bei Verdacht oder Auftreten eines Computer-Virus 35
5.1.1 Viruswall 35
5.1.2 E-Mail-Server ... 35
5.1.3 Nicht-vernetzte IT-Systeme ... 35
5.1.4 Vernetzte Endgeräte und Server ... 35
5.2 Alarme 35
5.2.1 Viruswall http - Virenalarm ... 35
5.2.2 Viruswall E-Mail - Virenalarm ... 35
5.2.3 Viruswall Content-Filter ausgehende E-Mail ... 35
5.2.4 NAV für Exchange - Virenalarm ... 35
5.2.5 NAV auf PC-Endgeräten und Servern - Virenalarm ... 35
5.2.6 IDS – Angriff auf pot. Schwachstelle ... 35
5.3 Benutzerhandbuch des Computer-Viren-Suchprogramms 35

1. Schutzbedarfsanalyse

1.1 Vorbemerkung

Dieses Virenschutzkonzept wurde nach Maßgabe des IT-Grundschutzhandbuches 2002 des Bundesamtes für Sicherheit in der Informationstechnik (BSI) erstellt. Die aufgeführten Maßnahmen und Regelungen, in den Überschriften durch eine M-Nummererierung gekennzeichnet, sind Mindestanforderungen des IT-Grundschutzes und werden größtenteils bereits seit mehreren Jahren im DPMA angewandt.

Ziel des Computer-Viren-Schutzkonzeptes ist die Unterstützung der Schaffung eines effektiven Computer-Virenschutzes für die IT-Systeme sowie die Dokumentation aller diesbezüglichen Entscheidungen.

Die Gesamtheit der enthaltenen organisatorischen Regelungen hat verbindlichen Charakter, so dass Verstöße gegen die Inhalte zu arbeits- oder disziplinarrechtlichen Konsequenzen führen können.
Das Konzept ist eine Grundlage für das weitere Vorgehen und sollte insbesondere beim Abschluss von Dienstvereinbarungen über die Nutzung von Intranet- und Internetdiensten, bzw. E-Mail, berücksichtigt werden. In diesen Dienstvereinbarungen können unter Berücksichtigung der hervorgehobenen Sicherheitsbelange des DPMA die notwendigen datenschutzrechtlichen Regelungen einfliessen.

1.2 Abhängigkeit des DPMA vom IT-Einsatz

Im DPMA sind mittlerweile über 95 % der Arbeitsplätze mit PC-Systemen ausgestattet, die Netzwerkzugang haben. In diesem Umfeld können Computerviren und andere Software mit Schadenswirkung auftreten und sich über das Netzwerk verbreiten. Dadurch kann der Datenbestand und die Arbeitsfähigkeit des Amtes gefährdet werden.

1.3 Beschreibung des Gefährdungspotentials

Seit Mitte der 80er Jahre gibt es Programme mit Schadenswirkung, kurz „Computerviren“ genannt. Ihre Zahl und die Vielfalt der unterschiedlichen Wirkungsweisen hat stark zugenommen und die von ihnen verursachten Schäden überschreiten jährlich weltweit die Milliardengrenze.

Computerviren haben zwei wesentliche Bestandteile:
- Sie beinhalten einen Programmteil, der eine Reproduktion (Ausbreitung) verursacht und
- ein zweiter Programmteil soll eine „unerwünschte Wirkung“ verursachen. Dies kann eine „Scherzfunktion“ sein, kann aber auch die Zerstörung von Daten und installierten Programmen zur Folge haben.

Grundsätzlich versucht der Programmierer eines Computervirus sein Programm zu verstecken, d.h. der Virus braucht ein „Wirtsprogramm“ oder ein Dokument, in das er eingebaut wird. Hierin liegt auch die eigentliche Gefahr für die Ausbreitung von Computerviren: Sie bleiben lange unentdeckt und können sich schnell ausbreiten und Schäden verursachen.

Computer-Würmer hingegen breiten sich über Peer-to-Peer Verbindungen (direkte Netzkommunikation) aus. Sie nutzen hierbei Schwachstellen des Betriebssystems, um sich in laufende Prozesse „einzuhängen“. Sind sie erst einmal ablauffähig im Arbeitsspeicher des Wirtssystems, versuchen sie weitere Rechner im Netzwerk zu infizieren. Es tritt ein „Schneeball-Effekt“ ein, welcher zum Zusammenbruch jeglicher Netzwerkkommunikation

führen kann. Um auch nach einem Neustart des Rechners wieder aktiv werden zu können, versuchen Würmer Dateien auf dem infizierten System abzulegen. Häufig sind Würmer in der Lage, jene Prozesse auf dem System anzuhalten, die einen Virenschutz realisieren sollen, so dass Würmer (und auch Trojaner) häufig, trotz installiertem Virenschutzprogramm, unentdeckt bleiben und sich verbreiten können. Es ist daher zwingend notwendig, ein möglicherweise betroffenes IT-System gründlich auf Fremdsoftware, unbekannte Dienste oder Run-Keys in der Registry zu überprüfen.

Wurm-Programme können zwar effizient durch eine Firewall gestoppt werden, es sind jedoch auch Kombinationen aus Viren und Würmern bekannt. Über ein Virus-Programm erfolgt bspw. die Ausbreitung per E-Mail, erreicht die E-Mail das Zielsystem und wird vom Anwender geöffnet, so wird der Wurm-Teil aktiviert, der dann das interne Netzwerk angreifen kann.

Mit Antivirenprogrammen können bereits bekannt gewordene Computerviren entdeckt werden. Ähnlich wie ein genetischer Fingerabdruck lässt sich auch ein von einem Virus infiziertes Programm erkennen. Neue oder bislang unbekannte Computerviren bleiben jedoch unentdeckt. Verschlüsselte Dateien oder verschlüsselte Web-Verbindungen (https) können ebenfalls von Virenscannern nicht überprüft werden und stellen daher ideale Ausbreitungswege dar.
Daraus folgt: **Der Einsatz von Antivirenprogrammen ist nur eine Schutzmaßnahme.** Umsichtiges Verhalten der IT-Nutzer ist ebenso unerlässlich.
Zusätzlich müssen Regeln für die Internet-Nutzung und die sachgemäße Verwendung von E-Mail bestehen, sowie weitere technische Maßnahmen zur Früherkennung von potentiellen Schadenswirkungen vorhanden sein. Die regelmässige Analyse der eingesetzten IT-Systeme auf Schwachstellen stellt ebenfalls eine wesentliche Sicherheitsmaßnahme dar.

Waren die ersten Computerviren noch in ausführbaren Programmen versteckt (.exe - Dateien), so benutzte die nächste Generation Treiber für Drucker oder Bildschirmschoner.
Eine große Gefahr geht von Computerviren aus, die auf Basis der Makrofunktionalitäten der Microsoft-Produkte konstruiert werden (Word-Makros oder Scripts die an E-Mails angehängt und automatisch beim Öffnen der Dokumente ausgeführt werden). Diese Computerviren „reisen“ mit ausgetauschten Dokumenten und im Zeitalter der elektronischen Post können sich Computerviren innerhalb kurzer Zeit weltweit ausbreiten (siehe „I love you“).

Eine weitere Art der digitalen Schädlinge versteckt sich auf Web-Seiten. Ruft ein Anwender im Internet eine bestimmte Web-Seite auf, so wird mit dem übertragenen HTML-Code auch bspw. Java-Script (oder anderen aktiven Code) auf den Browser des Zielsystems übertragen. Dieser aktive Code ist so konstruiert, dass er unter Ausnutzung von Schwachstellen des Browsers oder des Betriebssystems sich direkten Zugriff auf das Dateisystem des Zielrechners verschafft. Es werden dann Programme mit Schadenswirkung (Trojaner) installiert oder Daten aus dem Zielsystem ausgelesen. Ursprünglich wurde diese Technik von den Betreibern von Webseiten mit pornographischen Inhalten entwickelt, um so Einwahlprogramme (dialer) für teure 0190er Telefonverbindungen auf dem Anwender-PC zu installieren. Mittlerweile hat sich aber diese „Schadenstechnik“ auf weite Bereiche des Internets verbreitet, insbesondere wenn es um illegale Aktivitäten, wie bspw. Raubkopien, Musiktauschbörsen oder scheinbar kostenlose Software handelt.

Computerviren werden von Hackern heute auch eingesetzt um Daten zu entwenden. Nicht nur E-Mail-Listen von Geschäftspartnern verlassen unbemerkt das Unternehmen, sondern mit Hilfe von „trojanischen Pferden“ verschaffen sich Angreifer Passwörter, die den Zugang zu wichtigen IT-Komponenten schützen sollen. Häufig handelt es sich hierbei um sogenannte Share- oder Freeware Programme, mit zunächst nutzvoll erscheinenden Funktionen. Werden diese Programme installiert, so können sie unbemerkt im Hintergrund Daten aus dem Rechner auslesen und zum Programmhersteller übermitteln (Spy-Ware). Als Beispiel sei hier der attraktive Bildschirmschoner (Kaminfeuer) genannt, der, sobald er aktiv

wird, Dateien aus dem Rechner des Mitarbeiters an eine bestimmte Web-Seite im Internet überträgt.

Eine Vernichtung von Arbeitszeit verursachen die scheinbar wohlgemeinten Virenwarnungen, die nach dem Kettenbrief-Prinzip versandt werden. Diese „HOAXes" können schnell einige 1000 Mitarbeiter jeweils für einige Minuten von der Arbeit abhalten. Die Überprüfung der Echtheit der Warnungen sollte Spezialisten vorbehalten sein, die Warnung vor einem einzelnen, gerade besonders aggressiven Virus ist völlig überflüssig, wenn vom IT-Nutzer die grundsätzlichen Schutzregeln vor Computerviren **immer** eingehalten werden. Manche solche HOAXes verweisen auf bestehende Systemdateien, die vorgeblich den Virus beinhalten. Löscht der Anwender diese Dateien eigenmächtig, so kann er damit sein System außer Funktion setzen.

Computerviren wie „Melissa", „I love you", „Blaster" und „Sobig.F" haben weltweit Schäden in Millionenhöhe verursacht, letztendlich auf Grund unsachgemäßen Verhaltens von PC-Nutzern. Es ist zu beobachten, dass Computerviren gefährlicher werden und höhere Schäden verursachen.

Die nachstehende Übersicht gibt einen Überblick über Computerviren und Malware.

Malware	Beschreibung
Computerviren allgemein	Programme, die sich replizieren, indem sie andere Programme „infizieren", so dass diese eine (möglicherweise mutierte) Kopie des Virus enthalten. Computerviren können (müssen aber nicht!) eine „Nutzlast" enthalten, die Schädigungen oder andere, vom Benutzer unerwartete Aktionen durchführt. Der Begriff „Computerviren bezieht sich aber auch generell auf Programme mit Schadfunktionen („Malware"), also Computerviren im engeren Sinne, Würmer und Trojanische Pferde.
Programmviren (auch Dateiviren)	infizieren Programmdateien; beim Start des befallenen Programms verbreitet sich der Virus weiter.
Bootsektorviren	setzen sich im Bootsektor von Disketten oder Festplatten fest und werden beim Starten des Computers geladen.
Makroviren	werden mit den mächtigen modernen Makrosprachen, vor allem Visual Basic for Applications (VBA), programmiert und in Dokumenten abgespeichert. Wegen ihrer relativ einfachen Programmierung und der Dominanz weniger Produkte auch im Office-Bereich sind diese Computerviren sehr erfolgreich. Beim Austausch von Dateien (z. B. per Datenträger oder E-Mail) werden weitere PC-Systeme infiziert. Es gibt Dateiformate, die Makros nicht zulassen (z. B. Word: .rtf, Excel: .csv). Es wird empfohlen, Dateien in diesen Formaten weiterzugeben.
Würmer	unterscheiden sich von Computerviren dadurch, dass sie kein Wirtsprogramm benötigen und sich selbständig über Computernetze verbreiten. Würmer sind im allgemeinen in einer Skriptsprache geschrieben (Visual Basic Script, JavaScript). In letzter Zeit sind jedoch auch Würmer aufgetaucht, die Schwachstellen auf der Kommunikationsebene (Netzwerk) eines PCs nutzen, um sich zu verbreiten (z. B. Blaster). Diese Schädlinge werden erst nach der Infektion eines PCs durch einen Virenscanner erkannt und sind deshalb besonders aggressiv in ihrer Ausbreitung.
Trojanische Pferde	(auch „Trojaner" genannt): Programme, die angeblich oder tatsächlich etwas Nützliches tun, außerdem aber eine oder mehrere Funktionen ausführen, die weder erwartet noch erwünscht werden; z.B. scheinbar nützliche Freeware, die nach dem Start im Hintergrund Aktionen durchführt, etwa Datenzerstörung, PC-Fernsteuerung und Ausspähung

	von Daten. Im Gegensatz zu Würmern und Computerviren replizieren sich Trojaner (normalerweise) nicht. Eine Unterteilung der "Trojanische Pferde" kann erfolgen in: - legal und illegal, - Remotezugriff, Rootkits, Dropper (setzen Computerviren frei) und DDos-Agenten (z. B. Mail- und Ping-Attacken)
Ad-/Spyware	Bei der Installation von Programmen zusätzlich installierte Software, die während der Online-Verbindung Informationen über den Benutzer an den Hersteller oder Auftraggeber der Software schickt.
0190-Dialer	Programme, die über Modem oder ISDN eine Verbindung ins Internet herstellen und dabei eine 0190-Mehrwertnummer, meist zu einem extrem hohen Tarif (z.B. 1,86€ oder mehr), verwenden. Ist prinzipiell legal, allerdings wird mit diesem Geschäftsmodell meistens Schindluder getrieben. Um den Benutzer zu täuschen, verwenden 0190-Dialer oft ähnliche Täuschungsmechanismen wie Computerviren, Würmer und Trojaner.
Falschmeldung (Hoaxes)	Befallen nicht Maschinen, sondern Menschen. Meist falsche Virenwarnungen, die auf die Unsicherheit der Benutzer spekulieren. Immer werden die Benutzer aufgefordert, die Warnung weiterzuleiten; oft soll der Benutzer auch völlig virenfreie Systemdateien löschen. Hoaxes sind nicht harmloser als andere Computerviren, da sie durch die angerichtete Verwirrung hohen Schaden anrichten. Typische Bestandteile von Hoaxes sind: - Aufforderung, die E-Mail an möglichst viele Adressaten weiterzuleiten, - im Text wird erwähnt, dass es sich um einen ganz neuen unbekannten Virus handelt, der drastische Schäden anrichtet - es wird auf bekannte renommierte Organisationen Bezug genommen (z. B. Symantec, AOL, Microsoft etc.) - die originale E-Mail-Adresse bzw. Webadresse ist nicht verfügbar

Allen Programmen mit Schadenswirkung gemein ist ihre Ausbreitung über das Internet (Web-Seiten oder E-Mail). Die größte Gefährdung für ein Behörden- oder Firmennetz geht daher von der Bereitstellung des Internets am Arbeitsplatz aus.

Im Folgenden werden der Einfachheit halber alle Programme mit Schadenswirkung als Computerviren bezeichnet.

1.4 Schadensszenarien

Es ist bekannt, dass Computerviren Daten verändern oder gar löschen können. Dies ist natürlich sehr ernst zu nehmen, jedoch lassen sich zerstörte Daten durch ordnungsgemäß erstellte Sicherungskopien ersetzen. Voraussetzung dafür ist u. a. auch eine frühzeitige Erkennung von Computerviren. Computerviren können aber auch weitaus schlimmere Auswirkungen haben, die nicht immer sofort sichtbar sind.

So hemmen Computerviren den normalen Arbeitsablauf, wenn im DPMA ganze Netzwerke heruntergefahren werden müssen. Als Folge geht wertvolle Arbeitszeit verloren.

Manche Computerviren blockieren die Kommunikationskanäle im DPMA. So verbreiten sich die Computerviren Melissa oder ExploreZip über E-Mail und können derart viele E-Mails erzeugen, dass der E-Mail-Server sogar abstürzen kann. Auch wenn der Server der E-Mail-Flut gewachsen ist, ist es u. U. geboten, den E-Mail-Server aus reiner Vorsicht herunterzufahren.

Ebenso besteht eine Gefahr für vertrauliche Informationen. Der Computervirus Melissa kann Dokumente, die vertrauliche Informationen enthalten, an jeden Eintrag im Adressbuch weiterleiten.

Wenn Computer-Viren an Kunden oder Geschäftspartner weitergegeben werden, kann ein Imageschaden entstehen. Darüber hinaus können Imageschädigungen dadurch eintreten, dass Geschäftsprozesse oder einzelne Dienstleistungen nicht aufrechterhalten werden können und somit Verzögerungen entstehen.

Den wahrscheinlich größten Schaden durch Computerviren kann die Glaubwürdigkeit des DPMA nehmen. Wenn z. B. einem Geschäftspartner ein infiziertes Dokument geschickt wird, sieht er das DPMA möglicherweise nicht mehr als vertrauenswürdigen Partner an oder verlangt gar Schadenersatz vom DPMA. Durch manche Computerviren kann das DPMA auch in recht peinliche Situationen geraten und so seinen guten Ruf riskieren. Der Computervirus WM/Polypost legt beispielsweise Kopien von Dokumenten mit dem eigenen Namen bei der Usenet-Newsgroup alt.sex ab.

1.5 Potentiell betroffene IT-Systeme (M 2.155)

Alle IT-Systeme des DPMA werden durch den Netzwerkbereich über eine Datenbank verwaltet (Ref. 2.4.2). Die entsprechenden Systemattribute, wie bspw. Betriebssystem, sind der Datenbank zu entnehmen. Modems oder andere zusätzliche Kommunikations-schnittstellengeräte sind im DPMA nicht zugelassen. Da auf allen Windows-basierten System im DPMA die gleiche, zentral gesteuerte Virenschutzsoftware zum Einsatz kommt, ist eine gerätespezifische Differenzierung nicht notwendig.

1.5.1 Microsoft Windows Betriebssysteme

Durch Computerviren sind typischerweise alle IT-Systeme, die mit einem Microsoft Windows-Betriebssystem ausgestattet sind gefährdet. Gründe dafür sind in der starken Verbreitung von Microsoft-Betriebssystemen (Monokultur), einem sehr offenem Sicherheitskonzept in den Microsoft-Betriebssystemen mit vielen Sicherheitslücken und einer sehr hohen und ständig wachsenden Anzahl von Computerviren für diese Plattform zu sehen. Daher ist jedes IT-System mit einem Microsoft Windows Betriebssystem grundsätzlich mit einer Virenschutzsoftware auszustatten.

Microsoft Windows-Betriebssysteme sind im DPMA:

- Microsoft Windows NT 4 (in Ablösung) / 2000 / XP
- Micorsoft Windows Server 2000 / 2003

Eines dieser Betriebssysteme kann beispielsweise installiert sein auf:

- Arbeitsplatzrechnern
- Applikationsservern
- Gateway-Rechnern
- Notebooks / Laptops
- usw.

Mengengerüst Endgeräte:

- ca. 700 DEPATIS-PCs mit Windows 2000 (XP in Vorbereitung)
- ca. 1300 PCs aus den Verwaltungsbereichen, Marken, Geschmacksmuster, Personalverwaltung. Windows XP ab dem Rollout 1.8.2004
- ca. 50 PCs im Bereich der Telearbeit. Ausstattung wie Verwaltungs-PCs mit Windows XP. Transparent ans Netzwerk des DPMA angebunden. Ausbau auf 300 Geräte in Planung.

Mengengerüst windowsbasierte Server:

- ca. 25 davon 3 DCs, 1 Mailserver-Cluster, Softwareverteilserver, Anwendungsserver für SAP, Personalverwaltung, elektronische Anmeldung

1.5.2 UNIX- und LINUX-Betriebssysteme

Für den Bereich der UNIX- und LINUX-Betriebssysteme ist die Gefährdungslage im Zusammenhang mit Computerviren derzeit relativ niedrig einzuschätzen. Gründe dafür sind die niedrige Verbreitung dieser Betriebssysteme, die bei gleicher Plattform von verschiedenen Herstellern angeboten werden, einem grundsätzlich restriktiven Sicherheitskonzept und einer niedrigen, überschaubaren Anzahl von Computerviren. Im Regelfall kann daher auf die Installation einer Virenschutzsoftware verzichtet werden.

Wird das UNIX- / LINUX System auf einem Server eingesetzt, so sollte folgendes beachtet werden:

- Direkt auf dem Server sollten keine direkten Nutzeraktivitäten, die auf das Internet zugreifen (Web oder E-Mail) ausgeführt werden.
- Werden Updates aus dem Internet für den Server benötigt, so sind diese zunächst über ein Client-PC System herunterzuladen, das mit einem Computervirenschutz ausgestattet ist, und mit dem Virenschutzprogramm zu überprüfen. Erst hiernach darf die Software auf den Server übertragen und installiert werden. Software darf im
  Übrigen nur aus zuverlässigen Quellen (direkt von den Seiten der Hersteller der Software) heruntergeladen werden. Sekundär-Seiten (Spiegel) sind zu vermeiden, da die Original-Software möglicherweise durch unbefugte Dritte modifiziert worden sein konnte.

Betriebssysteme:

- True64 UNIX, davon 200 gleichartig konfigurierte Subserver der DEPATIS-Anwendung
- Linux SUSE, DEBIAN
- In Einzelfällen: Unix-Varianten anderer Hersteller

1.5.3 spezielle Anwendungssoftware

Auch IT-Systeme sind von Computerviren gefährdet, die mit Anwendungsprogrammen (wie Word oder Excel) ausgestattet sind, die durch Makro-Viren infiziert werden können. Makro-Viren werden mit den mächtigen modernen Makrosprachen, vor allem Visual Basic for Applications (VBA), programmiert und in Dokumenten abgespeichert. Wegen ihrer relativ einfachen Programmierung und der Dominanz weniger Produkte auch im Office-Bereich sind diese Computerviren sehr erfolgreich. Beim Austausch von Dateien (z. B. per Datenträger oder E-Mail) werden weitere PC-Systeme infiziert. Daher ist jedes IT-System, auf dem ein solches Anwendungsprogramme installiert wurden, grundsätzlich mit einer Virenschutzsoftware auszustatten.

1.5.4 Zentraler Fileserver

Der zentrale Fileserver (NAS) verwendet ein eigenes Betriebssystem, stellt aber auch eine Windowsemulation für den Filezugriff zur Verfügung. Auf dem Fileserver befinden sich die Home-Verzeichnisse der Windows-Anwender. Auf den Client-PCs ist der Echtzeitschutz aktiviert, der auch den Zugriff auf die auf dem Fileserver abgelegten Dateien überwacht, so dass auf den Einsatz eines zusätzlichen Virenscanners für das Filersystem verzichtet werden kann.

1.5.5 Andere Betriebssysteme

Sofern im DPMA weitere Betriebssysteme, als die oben aufgeführten eingesetzt werden, ist im Einzelfall zu entscheiden, inwieweit diese als potentiell gefährdet eingestuft werden

müssen. Diese Entscheidung ist nach der Empfehlung des IT-Sicherheitsmanagents zu treffen.

2. Erforderliche Schutzmaßnahmen

Aufgrund der IT-Strukturen des DPMA hat sich ein dreigeteiltes Computer-Virenschutzkonzept als sinnvolle und effektive Maßnahme entwickelt:

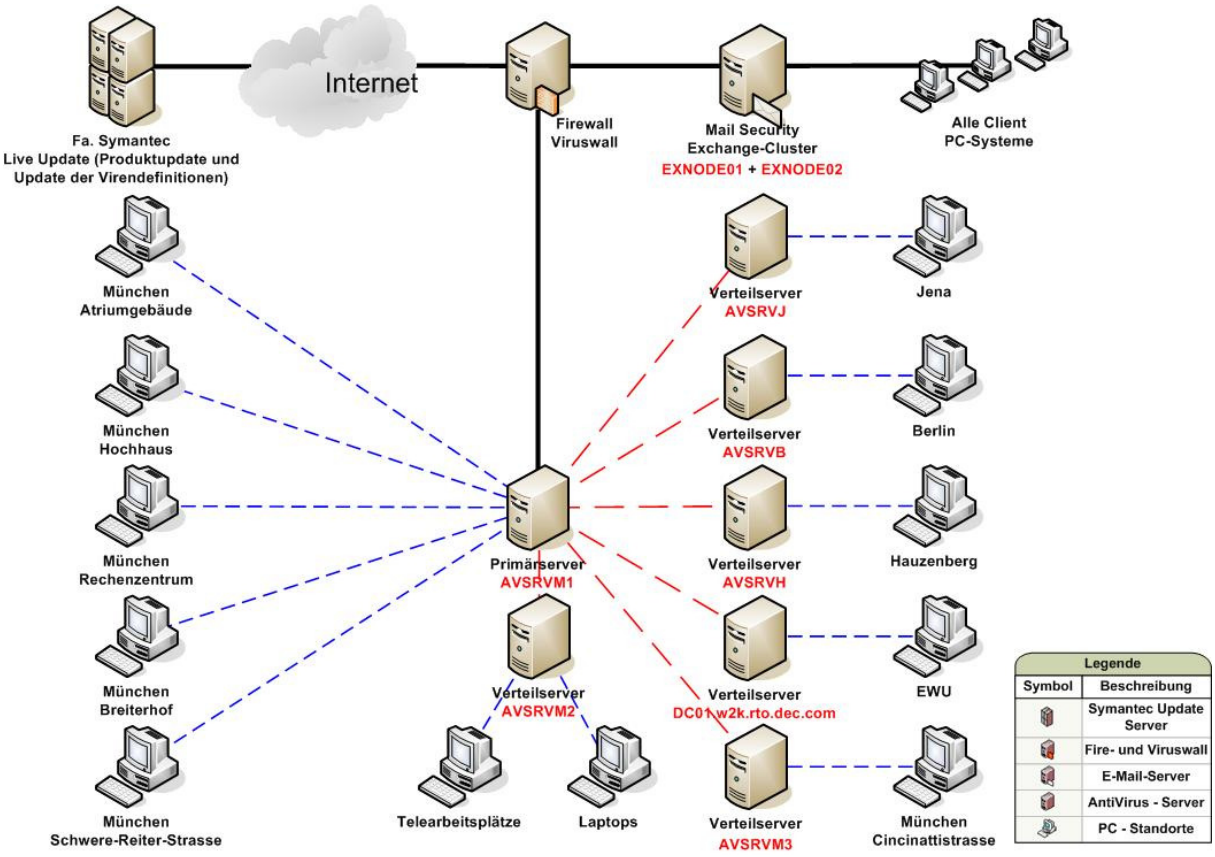

Abbildung 1: Computer-Virenschutz im DPMA

2.1 Computer-Virenschutz-Strategie (M 2.156)

2.1.1 Infektionswege

IT-Systeme können durch Viren auf verschiedenen Weisen infiziert werden. Nachfolgend sind die häufigsten Infektionswege aufgezeichnet. Die größte Gefahr besteht in der Öffnung der internen Netze nach außen, so dass die Gefahren insbesondere aus externer E-Mail-Kommunikation, dem Internetzugang und dem Austausch von Datenträgern resultieren. Das interne Netz kann die Ausbreitung im DPMA „begünstigen“.

Im DPMA wurden verschiedene Ebenen identifiziert, die grundsätzlich mit einem Computer-Virenschutz auszustatten sind. Diese Ebenen sind im Einzelnen:

- die Schnittstellen zwischen öffentlichem (externem) und privatem (internem) Netzwerk;
- E-Mail-Dienste;
  E-Mail dient immer öfter als Ersatz oder als Ergänzung zu anderen Bürokommunikationswegen. Mit Hilfe von Anhängen können Dateien effizient transportiert und E-Mail als Groupware-Lösung genutzt werden. Die angehängten Dateien können mit einem Virus infiziert sein und dieser kann durch das Medium E-Mail von außen in die Institution eingebracht und dort weiterverbreitet werden.

- Internet;
  Durch die immer größere Verbreitung von aktiven Inhalten auf WWW-Seiten entsteht die Gefährdung der Viren-Infektion. Momentan ist hiermit Java, ActiveX und Javascript gemeint, künftig könnten auch noch weitere Techniken hinzukommen. Auch können über Plug-Ins aus dem Browser heraus andere Programme gestartet werden. Auch Dateien und Programme, die aus dem Internet heruntergeladen werden, können infiziert sein. Gefährlich sind Schadprogramme, die sich über das Internet verbreiten und technisch so konstruiert sind, dass sie über eine nicht geschlossene Sicherheitslücke eines Programms (z. B. Browser oder Betriebssystem) direkt den Rechner infizieren.
- Internes Netz;
  Der interne Austausch von E-Mails und die Vernetzung der Rechner können die Ausbreitung eines Computer-Virus oder anderer Schadprogramme innerhalb der Institution herbeiführen. Sofern eine standortübergreifende Vernetzung vorhanden ist (z. B. Virtual Private Network) wird hierdurch die Verbreitung auch auf andere Standorte oder auch Fremdfirmen ermöglicht.
- PC-Systeme (mit der Schnittstelle „Datenträger“);
- Wechseldatenträger;
  Über Wechseldatenträger (z. B. Disketten, CDs, DVDs, USB-Sticks etc.) können Dateien oder Programme mit Computer-Viren IT-Systeme infizieren.
- Server (mit der Schnittstelle „Datenträger“);
- vernetzte PC-Systeme;
- mobile Geräte (z. B. Laptops);
  Sie werden teils im Intranet, teils mobil ohne Netzanschluss verwendet. Dadurch unterliegen sie besonderen Gefahren und sie stellen dadurch auch eine besondere Gefahr für das DPMA-LAN dar.
- vernetzte Server.

2.1.2 Einsatz von Virenscannern

Im DPMA ist dazu ein dreistufiger Computer-Virenschutz verwirklicht:

a) an der Schnittstelle vom externen zum internen Netzwerk (Viruswall):
   Prüfung des HTTP-, FTP- und SMTP-Datenstroms, sofern diese Verbindungen nicht verschlüsselt sind (Schwachstelle).
b) am Microsoft Exchange E-Mail-Server:
   Prüfung des gesamten internen und externen E-Mailverkehrs auf Dateianhänge mit Schadenswirkung,
c) auf den PC-Endgeräten und den Servern mit Microsoft Betriebssystemen:
   Prüfung des Datenaustauschs mittels Datenträger oder über Dateien, Anmerkung: Angriffe von Web-Seiten aus können nur dann mit dem Virenschutzprogramm nachgewiesen werden, wenn Dateien auf dem PC (z.B. temporäre Internet-Dateien) abgelegt werden. Erfolgreiche Angriffe, die speicherresident ablaufen (Würmer, Trojaner) können zum Zeitpunkt des Angriffes nicht detektiert werden (Schwachstelle).

Um eine klare überwachbare Schnittstelle zwischen internem und anderen externen Netzen zu haben, besteht im DPMA das strikte Verbot an IT-Systemen Modems oder andere Kommunikationskarten zu betreiben, wenn diese Geräte auch am internen Netzwerk angeschlossen werden. Diese Regelung gilt auch für Telearbeits- und Fernwartungsgeräte oder mobile Laptops (siehe „Abkürzungen und Konventionen - Querverweise [3]“). Sämtlicher Datenverkehr zu anderen Netzwerken ist grundsätzlich über das Firewall-System des DPMA zu leiten, um effizient und zentral auf Programme mit Schadenswirkung prüfen zu können.

Auch ein Virenscanner bietet keinen 100%igen Schutz gegen Computerviren und sonstige Malware. Computerviren können nur dann erfolgreich erkannt werden, wenn die entsprechenden Erkennungsmuster an der Viruswall, am Virenscanner des E-Mail-Servers

oder am lokalen PC-System bereits vorhanden sind. Diese Erkennungsmuster werden von einem Softwarehersteller sofort nach Bekannt werden eines neuen Virus erstellt. Die Virenerkennungsmuster der Virenscanner im DPMA werden dann automatisch aktualisiert.

Der Einsatz von Produkten unterschiedlicher Softwarehersteller kann sinnvoll sein, da die Virendefinitionsdateien von den Herstellern in unterschiedlichen Zyklen aktualisiert und bereitgestellt werden und sich die Erkennungsalgorithmen der Virensuchprogramme teils erheblich unterscheiden. Auch die Reaktionszeit zwischen der Entdeckung eines Computervirus bis zur Bereitstellung eines Erkennungsmusters kann herstellerabhängig verschieden sein.

2.1.3 Viruswall (M 2.157)

An der Viruswall (Firewall) erfolgt die Prüfung des HTTP-, FTP- und SMTP (E-Mail ein- und ausgehend)-Verkehrs auf Computerviren im Echtzeitmodus. Computerviren werden von der Software der Fa. Trend Micro automatisiert behandelt.

2.1.3.1 HTTP

Bei Computerviren im HTTP-Verkehr erscheint ein entsprechender Hinweis im Browser des Nutzers und die heruntergeladene Datei wird in ein Quarantäneverzeichnis überführt. Da nicht zweifelsfrei davon ausgegangen werden kann, dass auf dem Anwender-PC trotz der Sperrung durch die Viruswall weiterer Code mit Schadenswirkung zur Ausführung gelangte (dies konnte in einer Reihe von Fällen nachgewiesen werden), wird ein administrativer Alarm beim IT-Sicherheitsmanagement ausgelöst. Da der http-Datenstrom im internen Netz über einen Authentifizierungs-Proxy läuft und der Web-Zugriff somit anonymisiert ist, kann der Alarm zunächst nicht weiter ausgewertet werden. Um entsprechende Sicherungsmaßnahmen auf dem betroffenen Arbeitsplatzrechner durchführen zu können, muss über eine Datenbank, in der die Internetzugriffe temporär aufgezeichnet werden, der betroffene Rechner ermittelt werden (siehe auch Kap. 2.1.11.3). Das Verfahren bedarf gem. § 7 der Dienstvereinbarung über die Nutzung von Intranet- und Internet-Diensten im DPMA (siehe „Abkürzungen und Konventionen - Querverweise [4]“) jedoch einer Weisung der Amtsleitung, so dass eine zeitnahe Reaktion auf mögliche Schadensszenarien nicht möglich ist (Schwachstelle).
Bekannt gewordene Web-Seiten mit potentiellen Schadenswirkungen, wie z.B. auch Anbieter von Web-E-Mail (siehe Kap. 2.1.3.2), werden an der Firewall durch den Firewalladministrator gesperrt.

2.1.3.2 HTTPS

Verschlüsselte Datenverbindungen können nicht auf Computer-Viren überprüft werden. Sie stellen daher ein hochgradiges Risiko für das interne Netzwerk des DPMA dar.
Insbesondere verschlüsselte Web-Seiten mit individuellen Inhalten, wie z.B. bei Web-E-Mail Anbietern, sind bzgl. des Einschleusens von Computerviren sehr risikobehaftet. Daher wurden alle bekannten Web-Seiten von Anbietern des Web-E-Mail Dienstes an der Firewall gesperrt und von der Amtsleitung ein Verbot der Nutzung von Web-E-Mail erlassen.

A 1 Analyse der Protokolldateien auf Web-E-Mail Zugriffe

Die Einhaltung des Nutzungsverbotes von WebE--Mail ist wöchtentlich zu überprüfen. Hierzu sind die aus der Datenbank ermittelten URLs mit https (Port 443) Zugriffen auf möglichen Web-E-Mail-Verkehr zu analysieren. Werden Web-Mail Anbieter im Datenverkehr ermittelt, so sind:

a) die entsprechend qualifizierten URLs (login – Pages) durch die Firewall-Administration zu sperren;
b) Das Eskalationsverfahren bei Verdacht auf einen Sicherheitsverstoß gem. § 5 Punkt 1 der DV [4] einzuleiten (siehe „Abkürzungen und Konventionen - Querverweise [4]“).

Die Ergebnisse sind in einem Monatsbericht zu dokumentieren.

2.1.3.3 SMTP (E-Mail)

Sofern in einem E-Mail-Anhang ein entfernbarer Computervirus auftritt, wird dieser entfernt und der Datenstrom weitergeleitet. Andernfalls (Computervirus kann nicht entfernt werden) wird der virenbehaftete Anhang insgesamt aus der E-Mail entfernt und in ein Quarantäne-Verzeichnis abgelegt. Der Empfänger einer betroffenen E-Mail im DPMA wird automatisch mit einem entsprechenden Sicherheitshinweis benachrichtigt. Alle Quarantäneverzeichnisse werden regelmäßig gelöscht. In der Regel sind Computerviren, die im Quarantäne-Verzeichnis landen, nicht weiter zu beachten, da sie aus unseriösen Quellen stammen und für den Dienstbetrieb nicht relevant sind.
Auf Grund der hohen Zahl an täglich festgestellten eingehenden infizierten E-Mails (zwischen 100 – 1000) werden die ausgelösten administrativen Alarme nicht ausgewertet.

A 2 Trendanalyse der in eingehenden E-Mails festgestellten Viren

Einmal wöchentlich ist eine Trendanalyse der Virenmeldungen der Firewall für eingehende E-Mails durchzuführen. Festgestellt werden soll die aktuelle Verteilung auf unterschiedliche Virentypen. Die Ergebnisse sind in einem Monatsbericht zu dokumentieren.

Als weitere Schutzmaßnahme kommt ein Content-Filter in der Viruswall zum Einsatz. Dieser Filter ist so eingestellt, dass er grundsätzlich alle ausführbaren Dateianhänge, Audio- und Videodateien aus ein- und ausgehenden E-Mails entfernt. Diese Maßnahme musste implementiert werden, da häufig E-Mails mit neuen Computer-Viren ins interne Netz gelangten, bevor das entsprechend aktualisierte Virenschutz-Pattern veröffentlicht worden war.

A 3 Bearbeitung von Alarmen, die durch ausgehende E-Mails ausgelöst wurden

Ausgehende E-Mails mit ausführbaren Dateianhängen lösen einen administrativen Alarm aus, da sie Hinweise auf die Verletzung des „Verbotes der Nutzung nicht freigegebener Software“ liefern (weitere Ausführung in Kap. 3.1.2). Es ist das Eskalationsverfahren gem. § 5 Ziffer 1 der DV [4] einzuleiten (siehe „Abkürzungen und Konventionen - Querverweise [4]“).
Registrierte Alarme sind in einem Monatsbericht zu dokumentieren.

2.1.3.4 Rechtliche Aspekte

Im DPMA ist durch § 5 Ziffer 1 der Dienstvereinbarung über die Nutzung von Intranet- und Internet-Diensten im DPMA (siehe „Abkürzungen und Konventionen - Querverweise [4]“) die private Nutzung dieser Dienste ausgeschlossen. Daher stehen die an der Firewall / Viruswall des Amtes eingestellten sicherheitstechnischen Regelwerke im Einklang mit § 85 TKG und § 206 StGB. Die genannten Gesetze gestatten eine Veränderung des Datenstroms (Löschung von Dateien, Quarantäne), wenn die Sicherheit des IT-Betriebes durch Programme mit Schadenswirkung gefährdet ist (siehe auch § 13 BDSG).

2.1.3.5 Weitere Sicherheitsmaßnahmen

- Im http-Verkehr werden aktive Inhalte (ActiveX) ausgefiltert. Aktive Inhalte sind nur auf separaten – nicht an das interne Netz angeschlossenen – IT-Systemen zu ermöglichen.
- Aus dem Internet eingehende E-Mails, die eine „scheinbare" Absende-Adresse aus dem E-Mail-Adressbereich des Amtes (x.y@dpma.de) aufweisen, werden nicht zugestellt

A 4 Überprüfung von Sicherheitseinstellungen der Content-Filter

Die im Kap. 2.1.3.5 aufgeführten Sicherheitseinstellungen der Content-Filter sind einmal monatlich zu verifizieren. Das Prüfergebnis ist im Monatsbericht zu dokumentieren.

2.1.4 Zentraler E-Mail-Server MS-Exchange (M 2.157)

2.1.4.1 Virenschutz

Der zentrale E-Mail-Server (Cluster) ist mit einer Antivirenschutzsoftware der Fa. Symantec (Norton Antivirus für Exchange) ausgestattet. Auf dem E-Mail-Server erfolgt eine Prüfung im Echtzeitmodus der ein- und ausgehenden E-Mails und deren Anhänge auf Computerviren. Wird die Virendefinitionsdatei aktualisiert, so werden alle auf dem E-Mail-Server gespeicherten E-Mails und deren Dateianhänge auf Computerviren untersucht (Full-Scan).

Am E-Mail-Server werden Computerviren von der Software automatisiert behandelt. Sofern ein Computervirus entfernt werden kann, wird dieser entfernt und die E-Mail weitergeleitet. Andernfalls (Computervirus kann nicht entfernt werden) wird der Computervirus in ein Quarantäne-Verzeichnis abgelegt und am nächsten Tag manuell gelöscht. In der Regel sind Computerviren, die im Quarantäne-Verzeichnis landen, nicht weiter zu beachten, da sie aus unseriösen Quellen stammen und für den Dienstbetrieb nicht relevant sind.
Alle auf dem zentralen E-Mail-Server festgestellten Virenereignisse lösen einen administrativen Alarm beim IT-Sicherheitsmanagement aus.

A 5 Funktionsprüfung des Virenscanners auf dem Mailserver

Die beiden Virenscanner auf dem Mailserver-Cluster sind täglich zu überprüfen. Auf die Aktualität der Virenerkennungsmusters ist zu achten.
Die Quarantäneverzeichnisse sind zu analysieren, die Ergebnisse zu dokumentieren und die Verzeichnisinhalte einmal wöchentlich zu löschen.

2.1.4.2 Rechtliche Aspekte

Im DPMA ist durch § 5 Ziffer 1 der Dienstvereinbarung über die Nutzung von Intranet- und Internet-Diensten im DPMA (siehe „Abkürzungen und Konventionen - Querverweise [4]") die private Nutzung ausgeschlossen. Die Löschung, bzw. Verlagerung in einen Quarantänebereich, von vireninfizierten Dateianhängen aus E-Mails steht im Einklang mit § 85 TKG und § 206 StGB. Die genannten Gesetze gestatten eine Veränderung des Datenstroms (Löschung von Dateien, Quarantäne), wenn die Sicherheit des IT-Betriebes durch Programme mit Schadenswirkung gefährdet ist.

2.1.4.3 Weitere Sicherheitsmaßnahmen

Um die Ausbreitung von durch Würmern verursachten Massenmails zu verhindern, wurden
a) die Postfächer bzgl. ihrer Speichergröße auf 50 MB begrenzt und
b) die Zahl der Empfänger je versandter E-Mail auf 35 Adressaten beschränkt.

2.1.5 Nicht-vernetzte IT-Systeme (M 2.157)

Nicht-vernetzte IT-Systeme sind grundsätzlich mit einer Antivirensoftware auszustatten. Um die Aktualität der Virendefinitionsdateien, sowie die Konfiguration des Echtzeitschutzes und regelmäßige Vollprüfungen (mind. einmal wöchentlich) des IT-Systems muss sich der Benutzer eigenverantwortlich kümmern. Sofern Computerviren auftreten, muss der Benutzer diese eigenverantwortlich melden (Meldeweg siehe Kapitel 4.3), damit notwendige Gegenmaßnahmen ergriffen werden können.
Auf Grund des individuellen Betreuungsaufwandes sind nicht vernetzte PC-Systeme im DPMA die Ausnahme.

A 6 Bereitstellung von Virenschutzsoftware für nicht vernetzte PCs

Es ist ein Datenträger mit einem Virenschutzprogramm zu erstellen, das aktuelle Virenpattern zu integrieren und der Datenträger an den zuständigen Fachverantwortlichen zum Zwecke der Installation zu übergeben.
Die Übergabe ist zu dokumentieren, die regelmäßige Installation von aktuellen Virenpattern auf dem nicht vernetzten PC durch den Fachverantwortlichen ist monatlich nachzuprüfen.

2.1.6 Vernetzte Endgeräte (M 2.157)

Vernetzte Endgeräte (dies sind im Wesentlichen PC-Systeme und Server) sind grundsätzlich in das amtsweite zentrale Virenschutzsystem zu integrieren.

Zum Einsatz kommt die vom BSI für Bundesbehörden zur Verfügung gestellte Software der Fa. Symantec (Symantec Antivirus Corporate Edition) mit Softwareverteilserver und zentraler Konsolensteuerung.
Die Steuerung des amtsweiten Virenschutzsystems ist so konfiguriert, dass alle Dateien im Rahmen des Echtzeitschutzes geprüft werden. Bei PC-Systemen untersucht der Virenscanner im Echtzeitschutz Dateien bei Schreib- und Lesevorgängen auf Computerviren. Auf Servern untersucht der Virenscanner im Echtzeitschutz Dateien nur bei Schreibvorgängen (Performance). Wöchentlich werden PC-Clients am Freitag ab 11.45 Uhr und Server am Samstag um 23:59 Uhr vollständig auf Computerviren hin untersucht.

Wenn ein Computervirus gefunden wird, wird beim IT-Sicherheitsmanagement ein administrativer Alarm ausgelöst.

A 7 Dokumentationserstellung

Die Konfiguration von Symantec Antivirus Corporate Edition ist in Absprache mit dem IT-Sicherheitsmanagement vorzunehmen. Die Konfiguration ist zu dokumentieren. Die Dokumentation wird im IT-Sicherheitsmanagement bereitgehalten.

A 8 Funktionsprüfung von Symantec Antivirus Corporate Edition

Das zentrale System ist täglich auf korrekte Funktion zu überprüfen. Wesentliche Merkmale sind:

- Aktualität der Virenpattern auf dem Primärserver
- Aktualität der Clients

A 9 Bereitstellung der Virenschutzsoftware für die zentrale SW-Verteilung

Da im DPMA ein zentrales Softwareverteilwerkzeug eingesetzt wird, wurde das Virenschutzprogramm auch in die zentrale Verteilung als Paket aufgenommen. Im Falle eines Updates sind neue Pakete zu erstellen. Das IT-Sicherheitsmanagement testet die neue Version und unterstützt die mit der SW-Verteilung beauftragte Stelle im DPMA bei der Erstellung der neuen Pakete. Hierbei sind die standortbezogenen Sekundärserver des NAV-Systems in den Softwareeinstellungen des Virenschutzprogramms zu berücksichtigen.

2.1.7 Mobile Geräte (M 2.157)

Sie werden teils im Intranet, teils mobil ohne Netzanschluss verwendet und unterliegen dadurch besonderen Gefahren.

Im DPMA bestehen für Laptops zwei Einsatzmodelle:

a) „managed“ Laptops
b) „unmanaged“ Laptops

Geräte des Typs a) entsprechen in ihrer Softwareausstattung vernetzten PC-Systemen, d.h. sie sind auch an das zentrale Virenschutzsystem angeschlossen. Für diese Geräte besteht ein striktes Verbot sich direkt mit dem Internet zu verbinden. Im mobilen Einsatz kann über eine VPN-Verbindung die Ressourcen des DPMA genutzt werden. Eine Nutzung des Internets erfolgt dann über das Firewall-System des Amtes. Nimmt ein solches Gerät Kontakt mit den IT-Ressourcen des DPMA-Netzes auf, so erfolgt automatisch die Aktualisierung der Virenerkennungsmuster.

Geräte des Typs b) dürfen zu keinem Zeitpunkt an das DPMA-Netzwerk angeschlossen werden. Der Nutzer verpflichtet sich, den Softwarebestand und den Virenschutz auf diesem Gerätetyp selbst zu pflegen. Es ist eine Firewall zu installieren, die aktive Inhalte filtert.

Für beide Gerätetypen muss der Anwender ein Übernahmeprotokoll (Ref. 2.4.2) bestätigen.

2.1.8 Server (M 2.157)

siehe Kapitel 2.1.6

2.1.9 Geräte von Fremdfirmen

Geräte von Fremdfirmen dürfen nicht an das Netzwerk des DPMA angeschlossen werden.
Meist werden Geräte von Fremdfirmen auch in anderen Netzwerken betrieben, die aus Sicht des DPMA als unsicher eingestuft werden müssen (bspw. direkter Anschluss an das Internet oder dem Fremdfirmennetzwerk). Dies bedeutet für das DPMA ein erhöhtes Risiko für das Einschleusen von Computerviren wie Würmern.
Darüber hinaus ist bei Geräten von Fremdfirmen nicht sichergestellt, dass Konfiguration und Stand des Patchlevels dem DPMA-Standard entspricht.

2.1.10 Weitere Maßnahmen zur Gewährleistung eines flächendeckenden Virenschutzes (M 2.156)

Beim Einsatz der zentral gesteuerten Virenschutzsoftware für Microsoft Betriebssysteme wurde immer wieder beobachtet, dass die Schutzfunktion auf einzelnen Systemen nicht mehr vorhanden war. Ursache hierfür war häufig zu volle Festplatten und die unerlaubte Installation von nicht freigegebener Fremdsoftware.

A 10 Scannen des Netzwerkes zur Ermittlung inaktiver Virenschutzsoftware

Das Netzwerk ist mindestens einmal wöchentlich mit einer speziellen Funktion des Virenschutzsystems zu scannen, um Geräte ohne aktiven Virenschutz zu ermitteln. Hierdurch erübrigt sich das explizite Führen eines Katasters (Empfehlung IT-GSHB) der mit Virenschutzsoftware ausgestatteten Geräte.
Die detektierten Geräte ohne funktionstüchtigen Virenschutz, sofern es sich um Systeme mit dem Betriebssytemen von Microsoft handelt, sind unverzüglich in das zentrale Virenschutzsystem einzubinden.

2.1.11 Weitere Sicherheitssysteme zum Schutz gegen Computer-Viren (M 2.156)

Es muss betont werden, dass der Schutzmechanismus von Virenschutzprogrammen nur dann funktioniert, wenn ein Computervirus im Internet bereits erkannt wurde. Somit besteht immer noch ein gewisses Restrisiko, welches durch sachgemäßes Handeln der PC-Nutzer weiter minimiert werden muss (siehe Kap. 3.1.5 Schulung der IT-Benutzer (M 3.4, 3.5)).
Weitere Risiken ergeben sich durch die Internetnutzung, insbesondere dann, wenn Seiten aus „Graubereichen“ (bspw. Pornographie, illegaler Softwaretausch, Anfertigen von Raubkopien, Seiten mit rassistischen Inhalten) aufgerufen werden. Solche Seiten enthalten oft Schadenswirkungen (bspw. Dialer, Spyware), die durch Virenscanner nicht erkannt werden können.
Würmer, die sich über reine Netzwerkkommunikation (Peer-to-Peer) ausbreiten, umgehen das Echtzeitprüfsystem der installierten Virenschutzsoftware und können sich ebenfalls ungehindert ausbreiten. Erst wenn der Wurm sich resident auf die Festplatte schreiben will, um auch nach einem Neustart des Systems seine Ausbreitungsversuche fortzuführen, kann er u. U. von der Virenschutzsoftware erkannt werden. Dies ist aber häufig schon zu spät, da weitere IT-Systeme im Netzwerk schon infiziert wurden und der eintretende „Schneeballeffekt“ ein ganzes Netzwerk außer Funktion setzen kann.
Um diese real existierenden Restrisiken zu minimieren, werden weitere Sicherheitssysteme im DPMA eingesetzt.

2.1.11.1 Intrusion Detection System

Im DPMA wurde ein Intrusion Detection System (IDS) installiert. Ein interner Sensor überwacht den Netzverkehr im Bereich des Firewall-Systems. Versucht ein Wurm sich über das interne Netzwerk auszubreiten, so können seine spezifischen Signaturen durch das IDS erkannt werden, wenn die Datenpakete in das Netzsegment der Firewall gelangen. Das System kann jedoch nur dann einen Alarm auslösen, wenn die entsprechende Signatur des Schädlings bekannt ist und dieser Datenverkehr auf dem Netzwerk verursacht.
Die Erkennungsmuster werden vom Hersteller RealSecure (ISS) in regelmäßigen Abständen aktualisiert und automatisch installiert.
Ein Ausbau um weitere interne IDS-Sensoren scheitert an zwei Punkten:

- Die jährlichen Lizenzkosten für jeden weiteren Sensor sind sehr hoch (>10.000 Euro)
- Das DPMA-Netzwerk wird als geswitchtes Netzwerk betrieben. Die Datenübertragungsrate des Backbone beträgt je Einheit 1 GB/s. Für diese Transferraten ist keine wirtschaftlich vertretbare Sensorhardware verfügbar.

A 11 Funktionsprüfung des IDS

Das IDS ist täglich auf korrekte Funktion zu überprüfen:

- Aktualität des Updates
- Funktion der Sensoren
- Abruf der Ereignisse der letzten 24 Stunden
- Analyse des Event-Logs der zentralen Managementeinheit
- Überprüfung der Plattenkapazitäten
- Überprüfung des Zustandes der SQL-Datenbank

Monatlich ist die SQL-Datenbank über Wartungsfunktionen zu bereinigen und alle Daten, die älter als drei Monate sind, zu löschen.

A 12 Aktualisierung der Erkennungsmuster des IDS

Die Erkennungsmuster des IDS werden vom Hersteller bereitgestellt und automatisch vom IDS geladen. Nicht alle Erkennungsmuster betreffen die beim DPMA eingesetzten IT-Systeme. Relevante Angriffsmuster müssen mit einer eskalierten Alarmierungsstufe (bspw. per Mail) eingestuft werden. Es ist daher einmal wöchentlich eine Analyse der neuen Angriffsmuster und der im DPMA betroffenen Systeme durchzuführen und die entsprechenden Konfigurationen vorzunehmen.

A 13 Erstellung eines Monatsberichtes für das IDS

Im Rahmen der proaktiven Sicherheitsanalyse sind die registrierten Ereignisse des IDS auszuwerten und in einem Monatsbericht zusammenzustellen. Der Bericht beinhaltet auch eine Trendanalyse.

2.1.11.2 Trasher

Alle Datenpakete im internen Netzwerk, die keine gültige interne IP-Adresse aufweisen, werden automatisch auf ein Default-Gateway geleitet und dort analysiert. Die Ursachen für solche Datenpakete können vielfältiger Natur sein:

a) Fehlkonfigurationen von IT-Systemen
b) Fremdsoftware mit Spy-Funktionen
c) Computer-Würmer

Der Vorteil dieses Sicherheitssystems ist, dass kein spezifisches Erkennungsmuster zur Detektierung eines Netzwerkwurms vorhanden sein muss. Nachteilig ist, dass die Daten manuell interpretiert werden müssen und alle anderen Ursachen für Datenpakete mit ungültigen Fremdadressen im internen Netzwerk beseitigt werden müssen.

Die am Default-Gateway aufgezeichneten Daten werden einmal täglich in eine SQL-Datenbank importiert und können dann mit einer Reihe von Abfrageskripts analysiert werden.

A 14 Funktionsprüfung des Trasher-Systems

Das Trasher-System ist täglich auf seine Funktion zu überprüfen. Dies umfasst sowohl den auf einem Linux-System laufenden Sensor (Datengenerierung), als auch die Daten verarbeitende SQL-Datenbank. Die generierten Daten müssen in die Datenbank importiert werden und stehen dann zur Analyse bereit.

A 15 Analyse der Trasher-Daten

Die in der Trasher-Datenbank gespeicherten Daten müssen täglich analysiert werden. Hierbei müssen folgende Kriterien überprüft werden:

- Interne IP-Adressen, die hohen falsch adressierten Datenverkehr auslösen;
- Stark frequentierte Fremdadressen, die nicht zum Adressbereich des internen Netzes gehören;
- Portanomalitäten

Kritische Werte und Anomalien führen zu einem Alarm und dem entsprechenden Eskalationsverfahren.

2.1.11.3 Analyse der Internetverbindungen (http, https) – System PRPROTOK

Wie oben bereits erläutert wurde, lassen sich bestimmte Schadensprogramme, wie Würmer, Trojaner, Dialer und Spyware nur bedingt durch Virenscanner feststellen. Vielen dieser Schädlinge ist jedoch gemein, dass sie auffälligen Web-Verkehr (http) erzeugen. Dies kann sich durch periodische Zugriffe, hohe Zugriffszahlen auf bestimmten Web-Seiten, hohe Datenvolumina, Zugriffe auf Web-Seiten ohne URL (nur IP-Adresse) usw. äußern.

Häufig werden an der Firewall Alarme ausgelöst, die auf Web-Zugriffe zurückzuführen sind. Trotz der Blockade des virulenten Codes der Web-Seite können auch Schadenswirkungen auf dem Anwender-PC eintreten, so dass der ausgelöste Alarm in seinem Aufrufkontext analysiert werden muss, um ggfs. auf einem Anwender-PC weitere Sicherungsmaßnahmen auszuführen.

Um effizient solche Szenarien behandeln zu können, werden die Zugriffe auf das Internet in einer SQL-Datenbank aufgezeichnet. Da jede Schadenswirkung sich unterschiedlich darstellen kann, müssen die Daten manuell analysiert werden. Auf Grund der Datenmenge kann dies nur mit anonymisierten Stichproben durchgeführt werden. Wird eine „Auffälligkeit“ (Überschreiten von Grenzwerten, wie Zugriffszahl, Volumina, periodische Zugriffe, Aufrufzeiten einzelner Web-Seiten) festgestellt, muss der betroffene Anwender-PC ermittelt werden, um diesen näher untersuchen zu können.

Ziel ist es, zweifelsfrei festzustellen, ob die Ursache für das beobachtete Phänomen tatsächlich eine Fremdsoftware mit Schadenswirkung verursacht hat oder ob andere technische Gründe vorliegen. Die Untersuchung kann i.d.R. nur mit Unterstützung des betroffenen Anwenders erfolgen.
Erstes Ziel ist hierbei einen möglichen Schaden zu begrenzen, d.h., dass alle betroffenen IT-Ressourcen in eine sicherheitstechnische Analyse einzubeziehen sind.
Sollte sich bei der Analyse ergeben, dass der Alarm auch auf Grund einer missbräuchlichen Nutzung der IT-Ressourcen des Amtes durch einen Anwender verursacht wurde, so bedarf es zur weiteren Auswertung der Zugriffsdaten der Weisung der Amtsleitung. Das Verfahren ist in der „Dienstvereinbarung über die Nutzung von Intranet- und Internet-Diensten im DPMA“ festgelegt (siehe „Abkürzungen und Konventionen - Querverweise [4]“). Die Anlage 3 dieser DV beinhaltet eine Benutzerrichtlinie für die Nutzung des Internets mit einer Aufstellung der jeweils aktuell gültigen Sicherheitsregeln.

A 16 Funktionsüberprüfung des Systems PRPROTOK

Folgende Funktionen sind täglich zu überprüfen:

- Korrekter Ablauf der SQL-Auftragsdienste über den SQL-Enterprisemanager
- Zustand der Datenbank über den SQL-Enterprisemanager
- Überprüfung der ODBC-Verbindungen zum internen Proxyserver über den Aufruf der sespeicherten Prozedur „spPRXStatistics“

A 17 Analyse der Daten des Systems PRPROTOK

Folgende Analysen sind täglich und stichprobenartig durchzuführen:

- Durchführung von Analysen des Datenverkehrs nach den Kriterien Zugriffszahl, Volumina (insbesondere Upload), periodische Zugriffe, Aufrufzeiten einzelner Web-Seiten, Webseiten ohne URL
- Bei Feststellung „kritischer Ereignisse“ ist das Eskalationsverahren einzuleiten

A 18 Pflege des Systems PRPROTOK

Folgende Tätigkeiten sind monatlich durchzuführen:

- Löschung der Daten des abgelaufenen Monats binnen einer 30-Tage Frist
- Generierung einer neuen Konkordanzliste
- Pflege der gespeicherten Prozeduren und deren Datensicherung auf ein unabhängiges Speichermedium

2.2 Aktualisierung der Computer-Viren-Suchprogramme (M 2.159)

2.2.1 Viruswall

Die Aktualisierung der Virendefinitionsdateien (i.d.R. täglich automatisch), die Konfiguration und die Aktualisierung der Software werden vom Administrator der Viruswall durchgeführt.
Die Aufgabenkataloge sind im Handbuch „Firewall-System“ festgelegt.

2.2.2 E-Mail-Server

Die Aktualisierung der Virendefinitionsdateien, die Konfiguration und die Aktualisierung der Software werden vom Administrator des E-Mail-Servers durchgeführt.

2.2.3 Nicht-vernetzte IT-Systeme

Um die Aktualität der Virendefinitionsdatei sowie die Konfiguration des Echtzeitschutzes und regelmäßige Vollprüfungen (mind. einmal wöchentlich) des IT-Systems muss sich der Benutzer eigenverantwortlich kümmern.

2.2.4 Vernetzte Endgeräte

Die aktuellen Virendefinitionsdateien sowie die Konfiguration werden vom IT-Sicherheitsmanagement zentral bereitgestellt. Die Verteilung erfolgt netzwerkweit automatisch. Über die Konsole kann der Aktualitätsstatus des Virenschutzes jedes IT-Systems abgerufen werden und eine Funktionsprüfung durchgeführt werden.
Die Software wird von den zuständigen Administratoren aktualisiert.

2.2.5 Server

Siehe Kap. 2.2.4

A 19 Bereitstellung von aktuellen Virenpattern für Symantec Antivirus Corporate Edition

Für das amtsweite Computerviren-Schutzsystem Symantec Antivirus Corporate Edition ist täglich zu prüfen, ob neue Virenpattern verfügbar sind. Sofern diese nicht automatisiert in das System eingespielt wurden, sind sie manuell zu aktualisieren und bereitzustellen.

3. Regelungen

Die nachfolgend aufgeführten Regelungen und Maßnahmen sind dem IT-Grundschutzhandbuch des BSI entnommen und wurden für das Umfeld des DPMA entsprechend angepasst. Die Einhaltung dieser Regelungen und Maßnahmen ist für die Gewährleistung des IT-Grundschutzes zwingend erforderlich.

3.1 Regelungen zum Schutz vor Computer-Viren (M 2.160)

3.1.1 Nutzungsverbot nicht freigegebener Software (M 2.9)

3.1.1.1 Geltende Regelung

Der Punkt „Software“ der Benutzerrichtlinien für den ordnungsgemäßen Einsatz von Personalcomputern im Deutschen Patent- und Markenamt (siehe „Abkürzungen und Konventionen - Querverweise [1]“) und § 5 Ziffer 2 i. V. m. Anlage 3 der Dienstvereinbarung über die Nutzung von Intranet- und Internet-Diensten im DPMA – Anlage 3 (siehe „Abkürzungen und Konventionen - Querverweise [4]“) enthalten dazu die entsprechenden Regelungen und Hinweise. Diese Richtlinien besagen, dass es dem Endanwender grundsätzlich untersagt ist, eigenmächtig Software auf seinem PC-System zu installieren oder nicht freigegebene Fremdsoftware auszuführen.

3.1.1.2 Weitere technische Maßnahmen

- Durch eine eingeschränkte Benutzerrechtevergabe und mit Hilfe von Gruppenrichtlinien ist es dem Anwender technisch nicht möglich, Software mit Registrierungszugriffen zu installieren.
- Dateien und Programme dürfen nur von dazu Berechtigten von vertrauenswürdigen Quellen heruntergeladen werden. Das Herunterladen von ausführbaren Dateien aus dem Internet ist am Firewall-System / Proxy des DPMA zu sperren.
- Es ist für einen Dialerschutz zu sorgen, wenn Modems oder eine ISDN-Anlage/Karte genutzt werden. Kritische Nummernbereiche werden zentral an der ISDN-Anlage gesperrt.

3.1.1.3 Verfahren zur Softwarefreigabe

- Wird zusätzliche Software von einem Anwenderkreis benötigt, so wird die Anforderung über das Change-Board der IT-Planungsabteilung abgewickelt.
- Durch den IT-Betrieb wird eine „Verträglichkeitsprüfung“ zu den installierten Anwendungen durchgeführt. Das IT-Sicherheitsmanagement ist in diese Prüfung mit einzubeziehen.
- Nach der Durchführung von Tests durch eine „Friendly User – Group“ wird die Software dann für den allgemeinen Einsatz freigegeben. Die freigegebene Software wird über das zentrale Softwareverteilungswerkzeug auf den PC-Systemen installiert. Das Verteilungswerkzeug beinhaltet über seine Depot-Funktion eine Versionskontrolle (net-inventory).
- Eingesetzte Software wird über das Lizenzmanagement registriert.

3.1.1.4 Information der Endanwender

Im Rahmen der Öffentlichkeitsarbeit des IT-Sicherheitsmanagements wird in regelmäßigen Abständen an das Nutzungsverbot von nicht freigegebener Software erinnert (Hausnachrichten, DPMA-Aktuell).

3.1.2 Überprüfung des Einsatzes nicht freigegebener Software (M 2.10)

3.1.2.1 Stichprobenprüfung

Um Verstöße gegen das Verbot der Nutzung nicht freigegebener Software feststellen zu können, ist eine regelmäßige Überprüfung des Software-Bestandes notwendig. Da die Zahl der IT-Systeme sehr groß ist, wird eine stichprobenartige Überprüfung durch das Lizenzmanagement durchgeführt. Die Ergebnisse der Überprüfung werden dokumentiert, um auch Wiederholungsfälle feststellen zu können.
Sollte bei der Überprüfung nicht freigegebene Software gefunden werden, so wird die Entfernung veranlasst. Um diese Überprüfung durchführen zu können, wird dem Lizenzmanagement die entsprechende Befugnis durch die Amtleitung erteilt.
Festzulegen sind ferner:

- Turnus und Anzahl der Stichproben zur Überprüfungen des Softwarebestandes,
- Regelung zur Verfahrensweise bei festgestellten Verstößen.

A 20 Stichprobenprüfung durch das Lizenzmanagement

Das Lizenzmanagement führt vierteljährlich Überprüfungen des Softwarebestandes durch. Dabei sind jeweils zwei Prozent des Softwarebestands per Stichprobe zu überprüfen. Verstöße gegen Lizenzbedingungen sind aufzuklären.

3.1.2.2 anlassbezogene Prüfungen

Werden an den Sicherheitssystemen des DPMA Alarme (bspw. Virenschutzkomponenten, IDS, Firewall, Viruswall, Verletzung des Verbots des Versandes von ausführbaren Dateien per E-Mail, Ausfall der Virenschutzsoftware) ausgelöst, die Rückschlüsse auf den Einsatz nicht freigegebener Software zulassen, so kann das IT-Sicherheitsmanagement gem. § 13 Abs. 1 BDSG (Erforderlichkeit) zur Vermeidung möglicher Schäden unverzüglich eine Überprüfung der betroffenen Systeme durchführen. Besteht nach einer ersten Überprüfung der Verdacht auf einen Sicherheitsverstoß (Missbrauch), so wird gem. § 7 Abs. 2 der Dienstvereinbarung über die Nutzung von Intranet- und Internet-Diensten im DPMA (siehe „Abkürzungen und Konventionen - Querverweise [4]“) verfahren.

3.1.3 Dokumentation der Veränderungen an einem bestehenden System (M 2.34)

Für jedes Serversystem ist ein Betriebshandbuch / eine Dokumentation zu erstellen, aus der die Informationen über die installierte Software (einschließlich Version, Updates und Patches) zu entnehmen ist.
Für PC-Endgeräte ist auf Grund der hohen Anzahl der im DPMA eingesetzten Geräte keine individuelle Dokumentation zu führen. Installationsdaten können dem eingesetzten Softwareverteilungswerkzeug entnommen werden.

3.1.4 Informationsbeschaffung über Sicherheitslücken der Systeme (M 2.35)

A 21 „Bug-Traq“ - ing

Das IT-Sicherheitsmanagement wertet täglich die Beiträge einschlägiger Newsforen (CERT, BugTraq, Symantec) aus und überprüft, ob IT-Systeme des DPMA von den gemeldeten Schwachstellen betroffen sein könnten. Ist ein Sicherheitsupdate für die betroffenen Systeme verfügbar, so wertet das IT-Sicherheitsmanagement die für das DPMA bestehenden Risiken aus und veranlasst eine entsprechend priorisierte Aktualisierung der installierten Software.

3.1.5 Schulung der IT-Benutzer (M 3.4, 3.5)

- Programmschulungen sind über den Vorgesetzten beim Referat für Aus- und Fortbildung zu beantragen.
- IT-Sicherheitsbelehrungen werden vom IT-Sicherheitsmangement für neueingestellte Mitarbeiter oder anlassbezogen (bspw. bei Sicherheitsdefiziten) durchgeführt.

3.1.6 Nutzung der BIOS-Sicherheitsmechanismen (M 4.84)

Die Boot-Reihenfolge ist so eingestellt, dass nur von der Festplatte gestartet werden kann. Alle anderen boot-fähigen Geräte wurden im BIOS deaktiviert. Das BIOS ist mit einem, dem Anwender nicht bekannten, Passwort geschützt.

- **IT-Systeme, die an die zentrale Softwareverteilung angeschlossen sind:**
  Boot-Reihenfolge: Netzwerk, Festplatten, ~~Wechseldatenträger~~
- **alle anderen IT-Systeme:**
  Boot-Reihenfolge: Festplatten, ~~Wechseldatenträger~~

Bei allen moderneren Client-PCs enthält das BIOS eine Virenschutzfunktion, die aktiviert ist.

3.1.7 Erstellen einer Notfall-Diskette (M 6.24)

Sofern IT-Systeme an die zentrale Softwareverteilung angeschlossen sind oder in einem Clone-Verfahren erstellt wurden, kann auf das Anlegen einer Notfall-Diskette verzichtet werden. Die Daten des Nutzers sind auf einem Netzlaufwerk abzulegen (siehe „Abkürzungen und Konventionen - Querverweise [1]“). Dieses Netzlaufwerk (Fileserver) wird regelmäßig im Rahmen eines Backup-Plans gesichert.

Für alle anderen IT-Systeme (z. B. Server) sind Notfall-Disketten, geeignete Boot-CDs, Images oder Systemspeicherungen zu erstellen.

3.1.8 Maßnahmen bei nicht-resident virenschutzkontrollierten IT-Systemen

Es dürfen grundsätzlich keine IT-Systeme ohne residenten Virenschutz betrieben werden (dies schließt Laptops mit ein).

Anmerkung:
Erfolgt auf einem IT-System der Einsatz eines aktuellen residenten Computer-Viren-Suchprogramms (also eines Programms, das permanent im Hintergrund läuft), wird sichergestellt, dass ein infiziertes Programm nicht ausgeführt oder eine Datei mit einem Makro-Virus nicht geladen werden kann. Die Kontrolle der Schnittstellen am Endgerät übernimmt das residente Suchprogramm. Dadurch wird gewährleistet, dass eine Übertragung auf das IT-System nicht erfolgt. Ausnahme bilden hierbei aber Würmer, die sich über direkte Peer-to-Peer Verbindungen über das Netzwerk ausbreiten, da diese Würmer erst nach einer Weiterverbreitung Dateien im Dateisystem des infizierten PCs ablegen. Ferner sind solche Würmer auch in der Lage, die Echzeitprüfdienste von Virenschutzprogrammen auszuschalten.
Der ausschließliche Einsatz nicht-residenter Computer-Viren-Suchprogramme (die nur durch explizites Starten des Programms durch den Benutzer aktiviert werden) empfiehlt sich nicht, da hierdurch heute kein wesentlicher finanzieller Vorteil mehr erzielbar ist, jedoch die Nachteile auf seiten des IT-Benutzers erheblich zunehmen, da er zuverlässig regelmäßig das Programm aktivieren muss.

3.1.8.1 Regelmäßiger Einsatz eines Computer-Viren-Suchprogramms

Dieser Abschnitt betrifft lediglich nicht-vernetzte IT-Systeme, auf denen andere Virenschutzprogramme zum Einsatz kommen, als auf den Vernetzten Systemen (SAV). Daher gilt Kap. 2.1.5 entsprechend. Alle anderen IT-Systeme mit Windows-Betriebssystemen werden von einem zentralen Virenschutzsystem verwaltet, auf dem regelmäßige Prüfungen konfiguriert werden.

3.1.8.2 Virenkontrolle bei Datenträgeraustausch und Datenübertragung

Datenträger sind mit einer aktuellen Antivirensoftware zu prüfen. Die Virendefinitionsdatei darf nicht älter als 7 Tage sein.

Durch eine entsprechende Konfiguration des zentralen Virenschutzsystems (Echtzeitschutz, Prüfung von Wechselmedien) ist diese Maßnahme erfüllt.

3.1.8.3 Prüfung eingehender Dateien auf Makro-Viren

Die Antivirensoftware ist so zu konfigurieren, das Makroviren im Rahmen der regelmäßigen Vollprüfungen eines IT-Systems geprüft werden.
Durch eine entsprechende Konfiguration des zentralen Virenschutzsystems (Prüfung auf Makroviren) ist diese Maßnahme erfüllt.

3.1.9 Datenaustausch (M 4.33, 4.44)

An der Firewall des DPMA werden im E-Mail-Verkehr alle Dateitypen, die ausführbaren Code enthalten können (Ausnahme .doc, .xls) ausgefiltert. Als weitere Maßnahme werden ein-, ausgehende und hausinterne E-Mails auf Computer-Viren überprüft (Viruswall, Virenscanner auf MSExchange, Virenscanner auf PC-Client).
Auf allen vernetzten windows-basierten Systemen ist der Echtzeitschutz aktiviert, der automatisch sowohl eingelegte Datenträger, als auch Dateien mit Makros überprüft.
Zusätzlich wird für den Datenaustausch die Formate .rtf und .csv empfohlen.

3.1.10 Regelmäßiger Einsatz eines Virensuchprogramms (M 4.3)

Alle vernetzten Systeme auf Basis von MS-Windows werden über das zentrale Virenschutzsystem gesteuert. Eine vollständige Prüfung der Festplatten der Client-Systeme erfolgt einmal wöchentlich am Freitag, bei Servern am Sonntag.

3.1.11 Regelmäßige Datensicherung (M 6.32)

Für die Server und das Filer-System des DPMA bestehen Datensicherungskonzepte.
Gemäß der „Benutzerrichtlinien für den ordnungsgemäßen Einsatz von PC-Systemen im DPMA“ sind alle Nutzer angehalten, ihre dienstlichen Daten auf einem Netzlaufwerk abzuspeichern. Für lokal gespeicherte Daten ist der Anwender selbst verantwortlich. Für solche lokalen Daten übernimmt das DPMA keine Gewährleistung für die Einhaltung der Datensicherheit.

3.1.12 Eingeschränkte Benutzerumgebung

Um zu verhindern, dass der Endanwender sicherheitsrelevante Einstellungen verändert oder sein System auf unzulässige Weise beeinflusst, werden folgende Maßnahmen umgesetzt:

- Der Endanwender hat nur eingeschränkte Benutzerrechte;
- Die Sicherheitseinstellungen der Internet-Optionen werden vom Amt vorgegeben und können vom Endanwender nicht verändert werden;
- Die Einstellmöglichkeiten für Bildschirmschoner werden für den Endanwender gesperrt. Es wird somit der Einsatz nicht freigegebener Bildschirmschoner verhindert. Schwachstelle: Bildschirmschoner, die nur durch eine EXE-Datei gestartet werden und keine Eintragung in die Registrierungsdatenbank vornehmen, können gestartet werden.

3.1.13 Abnahmeprüfung von Servern durch das IT-Sicherheitsmanagement

Neu installierte Server-Systeme müssen durch das IT-Sicherheitsmanagement abgenommen werden. Diese Regelung ist auch bei Abschluss von IT-Verträgen mit externen Partnern zu berücksichtigen.

A 22 Sicherheitsüberprüfung von neu installierten Serversystemen

Das IT-Sicherheitsmanagement führt eine Sicherheitsüberprüfung von neu installierten Serversystemen unter Einsatz von Netzwerkscannern durch. Ziel ist es:

- Die Zahl der aktiven Diensten auf ein notwendiges Minimum zu reduzieren;
- Schwachstellen in Diensten zu entdecken und Empfehlungen zur Beseitigung dieser zu geben (Patches, Update oder Ersatz);
- Den Zugriffsschutz auf die Dateisysteme zu überprüfen.

Die Ergebnisse sind zu dokumentieren und in regelmäßigen Abständen zu wiederholen. Hierbei ist darauf zu achten, dass das eingesetzte Scan-Programm über eine aktualisierte Schwachstellenliste verfügt..

3.2 Regelung der Verantwortlichkeiten

Von der Amtsleitung wurde dem IT-Sicherheitsbeauftragten in Personalunion die Funktion des zentralen Computer-Viren-Verantwortlichen übertragen. Der IT-Sicherheitsbeauftragte legt die IT-Sicherheitsanforderungen in Absprache mit der Amtsleitung fest.

Die Kernkompetenz für das Aufgabengebiet des Computervirenschutzes wurde in ein Sachgebiet des IT-Sicherheitsmanagement verlagert. Dieses Sachgebiet wird bei seiner Arbeit durch Ansprechpartner in den Administrationsbereichen unterstützt.

3.2.1 Ansprechpartner für Computer-Viren

Wenn Computerviren auftreten, die nicht vollständig automatisch durch das Virenschutzprogramm beseitigt werden können oder bei denen nach Art und Umfang spezielle Überprüfungen notwendig sind, dann werden manuelle Eingriffe notwendig. Um dabei Überschneidungen der Verantwortlichkeiten zu vermeiden, wurde eine Regelung definiert. Das IT-Sicherheitsmanagement definiert die notwendigen Schritte und Maßnahmen zur Virenbeseitigung und gibt diese an die für die Systeme zuständigen Fachbereiche zur Erledigung weiter. Die Fachbereiche melden die Erledigung an das IT-Sicherheitsmanagement.
Dem Sachgebiet „Virenschutz“ des IT-Sicherheitsmagments wurde von den Fachbereichen folgende Ansprechpartner benannt:.
(siehe: „Abkürzungen und Konventionen - Querverweise [7]“)

Bereich	Ansprechpartner	Vertreter	Bemerkung
IT-Sicher-heit	Herr Oberleitner	Herr Riem	IT-Sicherheitsmanagement
2.4.1	Herr Storch	Herr Dobmann	
2.4.2	Frau Asam Herr Birnkammer Fa. CMS Herr Hohenberger	Herr Seulen Herr Sohanpall Herr Hahn Herrn Haucke	Exchange Server APCs Viruswall Windows-Server
2.4.3	Herr Lauster, Fa. HP Herr Dr. Behler	Herr Dr. Reppermund	DEPATIS-PCs
2.5.1	Herr Dr. Ruggaber Herr Dr. Ruggaber	Herr Dr. Mieskes Herr Dr. Mieskes	 Projekt EISA
2.5.2	RL 2.5.2 Herr Jäger Herr Krauß Herr Lorenz Herr Plath Herr Leicht Herr Bulicke Herr Holzmann	Herr Jäger Herr Agurks Herr Jäger Herr Ilschner Herr Kutzbora Herr Leicht Herr Kutzbora Frau Mamsch Herr Karatanev	 Telearbeit Testzentrum Marken Jena Jena Jena Berlin Patentamt Online

2.5.3	Herr Dr. Staude Herr Mück	Herr Braun Frau Schmidrkal, Fa. HP	Elektronische Annahmestelle
4.1.1	Herr Steuer		PC-Systeme der Personalverwaltung (H4, 4.1, 4.1.1, 4.1.2)

Tabelle 1: Ansprechpartner für Computer-Viren

3.2.2 Verantwortlichkeit von Administratoren

3.2.2.1 Allgemeine Verantwortung von Administratoren

- Soft- und Hardware sind durch den Administrator möglichst so zu konfigurieren, dass ohne weiteres Zutun des Benutzers optimale Sicherheit erreicht wird. Default-Einstellungen sind zu prüfen und Default-Passwörter zu ändern. Die Programme sind sicher einzustellen und vorhandene Sicherheitsfunktionen zu aktivieren – z. B. Schutz vor Makro-Viren innerhalb von Office-Programmen.
- Das Abschalten der Sicherheitsfunktionen durch den Benutzer ist nach Möglichkeit technisch zu verhindern.
- Vor dem Einsatz ist neue Soft- und Hardware zu testen. Dabei sollten nach Möglichkeit Testsystem und Produktivbetrieb getrennt werden. Das Internet darf auf Produktivservern nicht benutzt werden. Ausnahme davon sind automatisierte Aktualisierungsmaßnahmen bei gesicherten Verbindungen.
- Hard- und Software muss vor dem Einsatz freigegeben werden. Softwareänderungen machen eine erneute Freigabe erforderlich.
- Das automatische Ausführen von Makros ist zu verhindern.
- Um Sicherheitslücken zu schließen, hat sich der Administrator regelmäßig über sicherheitsrelevante Patches, Updates oder sonstige Anleitungen zur Behebung – bspw. beim Hersteller oder in einschlägigen Informationsquellen – zu informieren.
- Es sind die von den Herstellern veröffentlichten Patches und Updates zu beschaffen – insbesondere für Viren-Schutzprogramme und andere sicherheitsrelevante Programme wie Browser und Betriebssystem – und auf dem jeweiligen IT-System zu installieren. Sind keine entsprechenden Updates oder Patches verfügbar, müssen zusätzliche Sicherheitsmaßnahmen (Installation von Sicherheits-Soft und Hardware) ergriffen werden.
- Wichtig ist, dass Patches und Updates – wie jede andere Software – nur aus vertrauenswürdigen Quellen bezogen werden dürfen. Zusätzlich sind diese mit Hilfe eines aktuellen Viren-Schutzprogramms zu prüfen, bevor ein Update oder Patch installiert wird.
- In jedem Fall muss dokumentiert werden, wann, von wem und aus welchem Anlass Patches und Updates eingespielt wurden, so dass sich der aktuelle Patchlevel des Systems jederzeit schnell ermitteln lässt.
- Bei der Installation von Patches ist insbesondere darauf zu achten, dass durch voreingestellt Parameter die bestehende Konfiguration des Computer-Viren-Schutzprogramms nicht verändert wird.

3.2.2.2 Systemadministratoren

- Installation einer aktuellen Antivirensoftware auf PC-Systemen und Servern;
- Softwareupdates der Virenschutzsoftware durchführen;
- Virenentfernung nach Aufforderung und Anleitung durch das IT-Sicherheitsmanagement;
- Tägliche Auswertung der Ereignis- und Systemprotokolldaten. Insbesondere hohe CPU-Auslastung und/oder Netzwerkverkehr könnten Indizien für Programme mit Schadenswirkungen sein. Es ist ein Konzept zu entwickeln, wie die Ereignis- und

Systemprotokolldaten effizient zusammengeführt und nach definierten Kriterien ausgewertet werden sollen. Datenschutzbelange bleiben unberührt.

3.2.2.3 Viruswall-Administrator

- Installation einer aktuellen Antivirensoftware;
- Softwareupdates der Virenschutzsoftware durchführen;
- Aktualität der Virendefinitionsdateien sicherstellen;
- Pflege des Alarmierungssystems.

3.2.2.4 E-Mail-Server-Administration

- Installation einer aktuellen Antivirensoftware;
  Anmerkung: Da Viren-Suchprogramme mit der Zeit ihre Wirksamkeit verlieren, muss eine regelmäßige Aktualisierung erfolgen (Update der Viren-Signaturen). Die Computer-Viren-Signaturen sind darüber hinaus zu gegebenen Anlässen, z. B. aufgrund neuer Viren, zu aktualisieren.
  - Softwareupdates der Virenschutzsoftware durchführen;
  - Aktualität der Virendefinitionsdateien sicherstellen;
  - Regelmäßige Pflege (Bereinigung) des Quarantänebereiches.

3.2.3 Verantwortlichkeit des IT-Sicherheitsmanagements

Das IT-Sicherheitsmanagement hat die Aufgabe, die vollständige Umsetzung und Einhaltung die Einhaltung dieses Virenschutzkonzeptes sicherzustellen.
Im Rahmen der proaktiven Tätigkeiten haben folgende Aufgaben einen besonderen Stellenwert:

- Analyse von Alarmen;
- Einleitung von Sofortmaßnahmen bei akuten Bedrohungen;
- Beobachtung und Auswertung von Computerviren mit Gefährdungspotential;
- Vorschlagen geeigneter Schutzmassnahmen gegen Computerviren, wie bspw. Einspielen von Sicherheitsupdates veranlassen;
- Aktualität der Virendefinitionsdateien für das amtsweite Virenschutzsystem sicherstellen;
  Anmerkung: Da Viren-Suchprogramme mit der Zeit ihre Wirksamkeit verlieren, muss eine regelmäßige Aktualisierung erfolgen (Update der Viren-Signaturen). Die Computer-Viren-Signaturen sind darüber hinaus zu gegebenen Anlässen, z. B. aufgrund neuer Viren, zu aktualisieren.
- in Zusammenarbeit mit den Administrationsbereichen das Einspielen von Softwareupdates der Virenschutzsoftware veranlassen;
- in Zusammenarbeit mit den zuständigen Administratoren Virenentfernung auf infizierten IT-Systemen vornehmen;
- bei IT-Systemen, die an das amtsweite Virenschutzsystem angeschlossen sind, wöchentlich einen Virensuchlauf durchführen.

3.2.4 Verantwortlichkeit des einzelnen IT-Benutzers

- Durch sachgerechte und umsichtige Nutzung der IT-Systeme die Infizierung von IT-Systemen durch Computerviren vermeiden;
- Einhaltung der „Benutzerinformation zur IT-Sicherheit“ und der Dienstvereinbarung zur „Nutzung von Intranet- und Internet-Diensten im DPMA“;
- notwendige Schulungen beantragen;
- Computerviren melden;
- Das IT-Sicherheitsmanagement bei der Analyse von Alarmen und der Beseitigung von von Programmen mit Schadenswirkungen unterstützen;
- bei nicht-vernetzten IT-Systemen ist der IT-Benutzer zusätzlich für die in Kapitel 5.3 aufgelisteten Aufgaben verantwortlich.

4. Vorgehen bei Virenverdacht

4.1 Verhalten bei Virenbefall oder -verdacht

Die wichtigste Regel, wenn ein Computervirus tatsächlich ein IT-System infiziert hat: **Keine Panik!** Panisches, unsachgemäßes Verhalten schadet oft mehr als der Computervirus selbst verursacht.

Sollte der Verdacht auf einen „Virusbefall“ bestehen oder sollte der Virenscanner einen Computervirus melden, so ist umgehend das Helpdesk (Telefon 2000) zu informieren. Dieses verständigt im Bedarfsfall den IT-Sicherheitsbeauftragten, damit dieser die Quelle des Computervirus ausfindig machen kann und ggf. notwendige Gegenmaßnahmen treffen kann. Eigenmächtige Aktionen des Anwenders können wichtige Hinweise auf den Infektionsweg des Computervirus zerstören. Nur wenn der Infektionsweg zweifelsfrei geklärt werden kann, kann eine weitere Ausbreitung, und somit größeren Schaden vermieden werden.

Es gibt verschiedene Symptome, die auf Computerviren hindeuten können. Computerviren erkennt man u. a. an folgenden Symptomen:

- unsinnigen Systemmeldungen;
- fehlerhaften Bildschirmanzeigen bzw. Bildschirmausgaben verändern sich von selbst;
- unerklärlichen Systemabstürzen;
- deutlich reduzierter Verarbeitungsgeschwindigkeit;
- rätselhaftem Verlust von abgespeicherten Dateien oder es erscheinen neue, unbekannte Dateien auf der Festplatte bzw. dem Netzlaufwerk;
- Dateigröße der Programme ändert sich;
- freier Platz auf Festplatte schrumpft schnell;
- häufige Aktivitäten der Festplatte (Anmerkung: schwaches Indiz);
- dauernde Übertragung von Daten beim Internetsurfen (Bildschirmsymbol blinkt);
- nach Booten von Diskette kann nicht mehr auf Festplatte zugegriffen werden;
- Dokumente zeigen oft Rechtschreibfehler oder werden verändert;
- es entsteht erhöhter Netzwerkverkehr, da der Virus / Wurm sich versucht auszubreiten;
- im Ordner „Netzwerk- und DFÜ-Verbindugnen“ ist eine unbekannte Verbindung zu sehen.

Generell ist immer zu beachten:

- Dateien unbekannter Herkunft und auch Dateien von bekannten Personen sollten immer mit Vorsicht behandelt werden;
- Das Herunterladen, Installieren und Ausführen von Bildschirmschonern, Spielen und anderen ausführbaren Programmen sowie Bild-, Video- und Musikdateien aus dem Internet und das interne Verbreiten auf Dienst-PC-Systemen ist nicht gestattet.

4.2 Vorgehensweise bei Auftreten eines Computer-Virus (M 2.158, M 6.22)

Grundsätzlich gilt folgende Vorgehensweise:

1. Alarm registrieren
2. Quelle (betroffene Systeme) identifizieren
3. Schadenswirkung identifizieren
   Eine Schadenswirkung kann immer dann identifiziert werden, wenn das alarmierende System das Schadensprogramm auf Grund von Erkennungsmustern erkannt hat. Der Klartextname kann dann in den Virenlexika der Antivirensoftware-Hersteller

nachgeschlagen werden. Wird ein Virenverhalten gemeldet (IDS, Trasher, auf Grund von Protokolldaten in der Internetprotokollierung), so muss das System unverzüglich einer eingehenden Untersuchung unterzogen werden.

4. Schaden begrenzen
   Wird das Programm mit Schadenswirkung nicht automatisch entfernt oder isoliert, so muss zur Vermeidung einer Ausbreitung über das Netzwerk unverzüglich weitere Schutzmaßnahmen eingeleitet werden. Mögliche Maßnahmen sind bspw.:
   - Die Trennung des oder der betroffenen Systeme vom Netzwerk des DPMA;
   - Die Trennung des oder der betroffenen Teilnetze vom Netzwerk des DPMA, wenn der Schaden nicht eindeutig zugeordnet oder eindeutig abgeschätzt werden kann;
   - Umfassende Information der zuständigen Systemadministratoren; Erläuterung: Manche Computer-Viren oder Würmer „kapern“ Benutzerrechte und versuchen unter der Kennung des Anwenders weitere Ausbreitungsversuche. Es ist daher unerlässlich, die zuständigen Systemadministratoren umfassend zu informieren, um ggfs. sofort auf weitere kritische Ereignisse im Netzwerk zu reagieren. Es kann hierzu notwendig sein, das betroffene Nutzerkonto, vom dem die Schadenswirkung ausging, zu sperren.
5. Programm mit Schadenswirkung entfernen
   Hierzu ist anzumerken, dass nicht alle Computer-Viren, Würmer und Trojaner von Virenschutzprogrammen automatisch entfernt oder isoliert werden können. Häufig sind manuelle Nacharbeiten notwendig, die Administrationsrechte und direkten Zugriff auf das betroffene System notwendig machen. Auf keinen Fall darf der Nutzer hier selbst aktiv werden.
6. Nachsorge
   Zur „Nachsorge“ wird am betroffenen IT-System nach der Virenentfernung über mehrere Tage einmal täglich ein vollständiger Virensuchlauf durchgeführt.

4.3 Meldewege bei Auftreten eines Computer-Virus

4.3.1 Allgemeine Regelung

Der IT-Sicherheitsprozeß endet nicht mit der Umsetzung von Maßnahmen, sondern es bedarf periodischer Kontrollen, die bei Veränderungen auch die Aktualisierung der erstellten IT-Sicherheitskonzepte bewirken. Auch die Reaktionen auf sicherheitsrelevante Ereignisse müssen geregelt werden, um den Schaden zu begrenzen und Wiederholungen zu vermeiden.

Trotz noch so wirksamer Sicherheitsmaßnahmen ist es unvermeidlich, dass es Ereignisse gibt, die Sicherheitsprobleme aufdecken oder nach sich ziehen. Auf jedes dieser Ereignisse muss so schnell und effektiv wie möglich reagiert werden. Außerdem muss aus solchen Vorkommnissen gelernt werden, wie man diese und ähnliche Probleme in Zukunft vermeidet. Das DPMA kann Nutzen aus solchen Ereignissen ziehen, indem es Schwachstellen identifiziert und Sicherheitsmaßnahmen verbessert, wo es nötig ist.
Sicherheitsvorfälle können zum Beispiel ausgelöst werden durch

- Benutzerfehlverhalten, das zu Datenverlust oder sicherheitskritischer Änderung von Systemparametern führt,
- Auftreten von Sicherheitslücken in Hard- oder Softwarekomponenten,
- Auftreten von Computer-Viren,
- Hacking von Internet-Servern oder internen IT-Systemen,
- Offenlegung vertraulicher Daten,
- Personalausfall oder
- kriminelle Handlungen (etwa Einbruch oder Diebstahl mit IT-Bezug).

Es wurde deshalb ein Schema entwickelt und mit Verfügung des Leiters der Hauptabteilung Informationstechnik vom 28.06.2000 (siehe „Abkürzungen und Konventionen - Querverweise [6]“) in Kraft gesetzt, in dem festgeschrieben wird, wie auf sicherheitsrelevante Ereignisse reagiert werden muss und welche Meldewege einzuhalten sind, um die Reaktionszeit und den Schaden zu begrenzen.

4.3.2 Meldewege bei Programmen mit Schadenswirkung

Sollte der Verdacht auf einen „Virusbefall“ bestehen oder sollte der Virenscanner einen Computervirus melden, so ist umgehend das Helpdesk (Telefon 2000) zu informieren. Das Helpdesk informiert im Bedarfsfall den IT-Sicherheitsbeauftragten, damit dieser die Quelle des Computervirus ausfindig machen und ggf. notwendige Gegenmaßnahmen treffen kann.

Ausgelöste Alarme der Sicherheitssysteme werden automatisch per E-Mail und teilweise per Nachrichtendienst an das IT-Sicherheitsmanagement geleitet.

Ergeben sich aus den Alarmmeldungen begründete Verdachtsmomente auf einen vorsätzlichen Sicherheitsverstoß oder auf Missbrauch der IT-Einrichtungen des Amtes, so wird gem. § 7 der Dienstvereinbarung über die Nutzung von Intranet- und Internet-Diensten im DPMA (siehe „Abkürzungen und Konventionen - Querverweise [4]“) weiter verfahren, d. h., dass die Amtsleitung eine Weisung zur Durchführung weiterer Auswertungen erteilen muss.

5. Hilfsmittel

5.1 Verhaltensregeln bei Verdacht oder Auftreten eines Computer-Virus

5.1.1 Viruswall

siehe Kapitel 2.1.3

5.1.2 E-Mail-Server

siehe Kapitel 2.1.4

5.1.3 Nicht-vernetzte IT-Systeme

siehe Kapitel 2.1.5

5.1.4 Vernetzte Endgeräte und Server

siehe Kapitel 4.1

5.2 Alarme

Bei den durch die Sicherheitssysteme des DPMA ausgelösten Alarmen werden nachstehend folgende Daten übermittelt:

5.2.1 Viruswall http - Virenalarm

Datum, Uhrzeit, aufgerufene URL, Name des Virus, IP-Adresse des internen Proxies

5.2.2 Viruswall E-Mail - Virenalarm

Datum, Uhrzeit, Absende- und Zieladresse der E-Mail, infizierte Datei, Virusname

5.2.3 Viruswall Content-Filter ausgehende E-Mail

Enthält die ausgehende E-Mail einen unerlaubten Dateianhang, so wird ein Alarm ausgelöst.
Daten:
Datum, Uhrzeit, Absende- und Zieladresse der E-Mail, Name des ausgefilterten Dateianhangs

5.2.4 NAV für Exchange - Virenalarm

Datum, Uhrzeit
Absende- und Zieladresse der E-Mail, Virusname werden über die Konsole abgefragt

5.2.5 NAV auf PC-Endgeräten und Servern - Virenalarm

Datum, Uhrzeit, Name des IT-Systems
Virusname und weitere Informationen zur Infektion werden über die Konsole abgefragt

5.2.6 IDS – Angriff auf pot. Schwachstelle

Datum, Uhrzeit und Angriffstyp
Quell- und Ziel-IP-Adressen, Ports und Informationen zum Angriffsverlauf werden über die Konsole abgefragt

5.3 Benutzerhandbuch des Computer-Viren-Suchprogramms

Die Benutzerhandbücher befinden sich bei:

Virenschutz-Komponente	Produkt	Ansprechpartner
amtsweiter lokaler Computer-Virenschutz	Symantec AntiVirus Corporate Edition	Herr Oberleitner, Ber. 2.0.2
Viruswall	Trend Micro	Herr Dr. Optitz, Ref. 2.4.2 Herr Hahn, Ref. 2.4.2
E-Mail-Server	Symantec Mail Security für Exchange	Frau Asam, Ref. 2.4.2 Herr Seulen, Ref. 2.4.2

Tabelle 2: Benutzerhandbücher